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

This project has received funding from the European
Union’s Horizon 2020 research and innovation
programme under Grant agreement No 857237

DOCUMENT INFORMATION

DOCUMENT	D5.1 – Concept, design and architecture of the interoperable marketplace toolbox
TYPE	Report
DISTRIBUTION LEVEL	Public
DUE DELIVERY DATE	30/09/2021
DATE OF DELIVERY	31/01/2022 (resubmission)
VERSION	V1.4
DELIVERABLE RESPONSIBLE	SENSI
AUTHOR (S)	WP5 Partners
OFFICIAL REVIEWER/s	VLF, INESC TEC, SENSI

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, Yncréa, 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
1.2	Milenko Tosic (VLF), Fabio Coelho (INESC TEC)	22/09/2021	Included Executive Summary for Policy Makers and a high-level description of the interoperability compliance check.
1.3	Eliana Valles (Sensinov), Milenko Tosic (VLF), Fabio Coelho (INESC TEC)	30/09/2021	Final version addressing EC's Review Report comments – ready for submission
1.4	Milenko Tosic (VLF), Fabio Coelho (INESC TEC), Eliana Valles (Sensinov)	31/01/2022	Final version addressing EC's Review Report 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	E-Redes
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
Amândio 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 Chris Caerts Enrique Rivero Puente	VITO
Milenko Tosic Dragan Boscovic Sasa Pesic	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.

HISTORY OF CHANGES

- Updates in executive summary – requested in review report.
  - Removed content not directly related to D5.1.
  - Reworked flow of the main message of the Interoperability Framework specification and envisioned impact.
  - Updated relevant dates to reflect on the project progress.
- Removed terminology table and section 1.5 – it is documented in D2.1 where all listed concepts are used and relevant for the reference architecture definition.
- Updates to the Section 4 – addressing review report comment on the lack of common approach.
  - introduced Figure 7 – Functional map of the Interoperability Framework and paragraph before the figure.
  - Reduced description of different interoperability levels in section 4.2.1.
  - Renamed section 4.2.2.
  - Removed old section 4.2.3 and introduced new section 4.2.3 with detailed specification of the semantic interoperability layer and its components as they are implemented in the Interoperability Framework.
  - Removed section 4.3.1 on service terminology. Not relevant for the Service Store specification.
  - Section 4.4 – introduced two new bullets for the role and application of smart contracts in P2P marketplaces.
  - Introduced section 4.6 on the role of blockchain technologies in the interoperability framework – addressing comment from review report.
- Updates to the Section 5 – addressing comment on the lack of common vision.
  - Added content and Figures 34/35 at the start of the section with “The InterConnect interoperability Framework as a common approach for building semantically interoperable ecosystems that are project pilots”
  - Updated per-pilot Figures showcasing how the Interoperability Framework is mapped onto each pilot.
- Updates in the Conclusion:
  - Updated “What are the main components of the presented Interoperability Framework architecture” to reflect on the updates in the section 4. Added last paragraph on the “centralized middleware” requirement discussion.
  - Updated dates in “What are the plans for implementing and validating the Interoperability Framework?” and reflected on workshops organized for the pilots.
  - Updated “How will the Interoperability Framework be utilized within the project?” and “How will wider public benefit from the Interoperability Framework?” to reflect on progress in developing and delivering Interoperability Framework. Updated Figure 44.
  - Added paragraph on service interoperability in “How do we know it will work?”.

Minor editing updates and typo corrections throughout the document. Some content changed from future tense to present or past tense to reflect on the fact that the Interoperability Framework has been developed and is now in deployment and validation phase.

EXECUTIVE SUMMARY

Important note *- Concept of Interoperable Marketplace Toolbox from the proposal is now InterConnect Interoperability Framework!*

Energy and IoT domain convergence through cross-domain semantic interoperability is at the forefront of the InterConnect project. D5.1 focuses on the **specification of key enablers for implementing semantic interoperability among digital platforms, services, and devices from both the Energy and IoT domains**. InterConnect introduces the **Interoperability Framework as a set of tools and software components allowing stakeholders to interconnect their semantically interoperable solutions into interoperable ecosystems**, which are the basis for developing innovative services, use cases and business models.

The Background

Most IoT systems and other digital services and platforms from the same domain are expected to be interoperable at a syntactic level. This means that they use the same communication protocol and common data formats. Interconnecting syntactically interoperable systems boils down to accepting the same data model.

Once syntactic interoperability is achieved, the next level is semantic interoperability. **Semantic interoperability is the ability that digital systems have, to exchange data with unambiguous, shared and agreed meaning.** The meaning of data is set in an ontology that is accepted by all parties participating in data exchange. Semantic interoperability is a requirement to enable semantic reasoning and knowledge inference, knowledge discovery, and data federation between digital systems. Semantic interoperability is one of the main enablers for the concept of data spaces. Semantically interoperable digital systems can establish **semantically interoperable ecosystems (examples of such systems are InterConnect pilots)**, where innovative services and applications, based on federated knowledge, can be built.

The InterConnect **Interoperability Framework** enables the creation of semantically interoperable ecosystems comprising digital platforms, devices, and services from both IoT and energy domains. The **SAREF ontology** and its extensions (standard and custom, project defined) are used within the InterConnect project as the shared vocabulary for digital platforms, services and devices from both domains covered by the project. The overall goal of the **established semantically interoperable ecosystems is to improve the integration of systems and services, allowing to more easily combine, swap, evolve them thus unlocking new features and capabilities addressing privacy concerns and ensure competitive market offering.**

This work is consistent with the best practices from the European IoT Platform Initiative projects[1] where solutions for interoperability and federation of IoT platforms were developed and validated. InterConnect **Interoperability Framework** extends the work achieved by these projects towards cross-domain (IoT and energy) semantic interoperability of platforms and services without intermediary, centrally hosted facilitating platform. The project will validate achieved semantic interoperability performance, scalability, and exploitation potential in seven large scale pilots and open calls.

The Innovative Contribution

The two main reasons why semantic interoperability is not established yet on a larger scale are:
1. Steep technology learning/mastering curve of a disruptive paradigm based on information dissemination rather than a one-to-one data exchange approach used today by digital systems

[1] https://iot-epi.eu/

(addressed with the InterConnect Interoperability Framework); 2. Agreeing business level interoperability between industrial leaders is hard (addressed by the project pilots).

Because of the difficulty to master technology and risks associated with retrofitting digital systems already in production, semantic interoperability is **usually facilitated by intermediaries**. Digital platforms acting as protocol proxies and data model mappers are provided by specialized stakeholders. Most of the commercial solutions and research and innovation projects tackling interoperability challenges choose this approach - providing a centralized platform to facilitate data exchange in a uniform manner. Challenges to this are: 1. Dependability on centrally hosted facilitators both technically and business wise; 2. Data needs to be processed by a 3rd party which opens new data and privacy protection risks; 3. Performance is dictated by capacity of the facilitating platform; 4. Accepting new technologies and standards depends on the facilitating platform operator; 5. Extending interoperability features needs to be supported and enabled by the facilitator; 6. End to end cybersecurity is limited by the security measures employed by the facilitating platform (the weakest link in a chain); 7. Hosting a dedicated digital platform as an interoperability facilitator reduces energy efficiency of the process as new hardware needs to be deployed specifically for this purpose. Based on these limitations, it is evident that a more **decentralized approach for enabling semantic interoperability is needed**.

If the technological challenge of achieving semantic interoperability is resolved and demonstrated by InterConnect's large-scale pilots in an efficient manner, there will be a **new and clear incentive for business level interoperability** to be pursued.

Based on the state of the art and our common findings, the project has established several key requirements for its cross-domain semantically interoperable ecosystems, namely:

- **Distributed facilitating platforms:** Semantic interoperability must not depend on a centrally hosted facilitating platform, but instead rely on a distributed manner among already existing digital platforms operated by stakeholders.
- **Interoperable (generic) adapters/connectors:** Semantic interoperability needs to originate at the stakeholder's side - system operators must perform an adaptation of their services and interfaces in line with interoperability goals defined for the interoperable ecosystem. Semantic interoperability enablers should be implemented as software artifacts which can be **easily integrated** into most digital systems. The enablers should be **configurable** so that they can support different ontologies, legacy interfaces and access control limitations dictated by business logic behind services. Moreover, adaptation must be **cost effective**, **based on standard practices** and **flexible enough** to support the evolution of service offerings. This adaptation **should not disrupt syntactic interoperability** capabilities of participating digital systems.
- **Ontology agnostic:** If possible, semantic interoperability enablers should be ontology agnostic so that systems can test and adopt different ontologies for different use cases.
- **Security, privacy, and trustworthiness:** Semantic interoperability and **should not have a negative impact on already established levels of cybersecurity and privacy protection**. Interoperability must be **trusted**, in the cybersecurity and data protection sense, and also in a sense that guarantees that all endpoints support the same interoperability logic and have the interoperability levels that they claim. To effectively manage privacy protection in end-to-end communication, **clear privacy protection jurisdictions** throughout the ecosystem must be established.
- **Multiple deployment options:** Distributed interoperability enablers must support **different deployment options** from instantiating interoperability enablers on different system levels of one digital platform (from device to cloud) towards centrally hosted enablers instantiated and managed by one or all stakeholders of the interoperable ecosystem.
- **Federated knowledge pools:** semantically interoperable ecosystems establish federated knowledge processes, which provide new capabilities in designing and operating services and

applications. There needs to be a clear trade-off between communication/data handling overhead for achieving interoperability on the one side and ability to receive requested information from a federated knowledge pool with a single query on the other side.

The Approach

We have **combined a bottom-up and top-down approach** when defining the Interoperability Framework.

The **top-down approach** was carried out by analysing other research projects and initiatives tackling the challenges of (semantic) interoperability. Specific focus was put on lessons learned from the **European IoT Platform Initiative** projects. Their experience in enabling semantic interoperability between IoT systems with centralized and distributed interoperability enablers proved to be valuable input for drafting the Interoperability Framework concept. Next, **standard reference architectures for IoT and energy domains** were analysed with the goal of identifying necessary technology bridges for enabling intra and inter domain interoperability while ensuring that reference architectures can be mapped onto interoperable ecosystems.

The **bottom-up approach** started with **analysis of the digital platforms provided by the project partners,** which must be made semantically interoperable, to be used as a basis for building interoperable ecosystems to be validated in the project pilots. Interfacing capabilities were assessed in detail to ensure that proposed interoperability enablers can be employed by platform operators without disrupting existing processes and business logic. Finally, we have analysed **interoperability requirements of all project pilots** to identify interoperability points to be established between participating digital systems and assess requirements for facilitating these interoperability points.

The InterConnect project aims at delivering an Interoperability Framework capable of bridging the integration gaps "within" and "between" the IoT and the energy domains.

The identified requirements (see the Contributions part) led to specification of the Interoperability Framework comprising:

- **Semantic interoperability layer** (using InterConnect ontology over SAREF) based on distributed enablers interconnecting all resources, platforms and services and enabling them to exchange data and instructions in a uniform and secure manner while relying on widely adopted interfacing technology (RESTful). Exchanged data is not stored or processed anywhere in between communicating parties.
- **Service Store** a catalogue of all interoperable services, including knowledge exploring capabilities, service testing sandbox and automated interoperability compliance tests, streamline onboarding of 3rd parties' services and systems to become part of the InterConnect ecosystem ensuring growth of the interoperable ecosystems and creation of new ones.
- DLT based **P2P marketplace enablers** allowing community-based energy and data trading use cases to be implemented in a way interoperable with project's ecosystem.
- **Configurable access control** and knowledge handling procedures so that stakeholders can maintain business logic behind their services.
- A **methodology** for building semantically interoperable ecosystem by instantiating and configuring Interoperability Framework enablers within and among digital platforms and services comprising the interoperable ecosystem.

The Interoperability Framework provides different means for instantiation from centrally hosted facilitator to distributed framework maintained by interoperable ecosystem stakeholders. The result is enabling components (services, devices, digital platforms) to interact with each other without having to know each other's local native API, but purely based on the knowledge of ontologies and what ontology (category) a component belongs to (e.g., forecaster service). Finally, the knowledge-centric interface made available by the Interoperability Framework, based on SAREF, becomes the **interoperable and common vision** that links all stakeholders in InterConnect, while not limiting the expressiveness nor the diversity of each party.

The Results

The Interoperability Framework was **publicly released in January 2022**. All software artifacts are available for download and instantiation, so that a completely independent interoperability ecosystem can be built by interested parties. Project partners are documenting their success stories and providing their interoperability adapters as example implementations and best practices to be followed by integrators who base their systems on the same/similar technologies - learn and do by example approach that benefits from the project's consortium diversity.

The Interoperability Framework is, at this stage, **targeting system integrators, service providers, device manufactures, application developers and digital platform operators** to help them achieve semantic interoperability in a cost-effective manner and unlocking the full potential of federated knowledge pools.

How do we know it will work?

Reason 1 - easing the technology uptake process will attract stakeholders to consider and test the technology and be onboarded into interoperable ecosystems.

The Interoperability Framework includes enablers for achieving semantic interoperability, ensuring a much more manageable technology uptake, and learning curve than "vanilla" semantic web solutions. This ensures that integrators can achieve full semantic interoperability with tool sets they are mostly familiar with and with enough deployment flexibility without disrupting their well-established practices.

Reason 2 - once onboarded, stakeholders will be motivated to maintain the achieved semantic interoperability.

The Interoperability Framework is specified so that it enables interoperable ecosystems to be established and to take full advantage of federated knowledge pools. The project consortium includes key stakeholders from IoT and energy domains. Pilots will establish large scale interoperable ecosystems. As the interoperable ecosystems are validated with innovative use cases, more stakeholders will be attracted to join them (i.e., via the cascade funding and other initiatives).

Interoperable ecosystems established with instances of the Interoperability Framework will be able to run innovative value-added services targeted towards key stakeholders from IoT and energy domains including end users. Pervasive deployment of the Interoperability Framework will create a building/community/city/region/Europe-wide semantically interoperable ecosystems where devices and home management systems will be able to automatically or on demand choose among plethora of interoperable services specifically tailored for a challenge at hand. Home and building management systems will be able to aggregate and offer valuable data (e.g., demand side flexibility) to the energy marketplace decision makers. Energy communities will be able to operate without 3rd party facilitators and federate with other communities and large prosumers to improve their competitiveness on a wider energy market.

Finally, the **InterConnect Interoperability Framework is defined to be ontology agnostic,** so it is applicable to other domains as well, not just IoT and energy. This opens possibilities for new cross domain challenges. During the project, **SAREF**-based semantic interoperability will be demonstrated and the framework will have a set of tools specifically tailored to **SAREF**.

The Interoperability Framework is one of the key resources of the project utilized in collaborative efforts with other European initiatives towards emergence of validated best practices and standards for cross-domain semantic interoperability.

As part of the **BRIDGE initiative**, the project promotes the Interoperability Framework as a toolset for establishing new and bridging existing interoperable ecosystems.

The Interoperability Framework is implemented to be in line with the Gaia-X specifications:

1. "The users always retain sovereignty over their data. So, what emerges is not a cloud, but a federated system that links many cloud services providers and users together." The Framework provides this for service providers - distributed semantic interoperability layer where service providers maintain full control over their data;

2. "Data Spaces represent a data integration concept without a central storage. Thus, data remains at its source and is only shared when needed." The Framework is used to establish distributed data spaces (interoperable ecosystems) with federated knowledge enabled through semantic interoperability and shared SAREF ontology.

[2]

Stronger alignment with the Gaia-X will be pursued and options for including the Interoperability Framework into the Gaia-X reference methodologies for building cross-domain data spaces will be investigated. This direction of Interoperability Framework impact creation goes towards strategy on building “Common European Energy Data Space”.

As part of the **Open DEI Energy**, the project contributes to the WG4 with the Interoperability Framework as a facilitator for building interoperable ecosystems and as an enabler for bridging different reference architectures represented by other projects.

[2] https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf

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
IF	Interoperability Framework
IFA	Interoperability Framework Architecture
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 "Digital Platforms and Marketplace" oversees the following activities and objectives:

- Establish semantic 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 on 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);
- Provide continuous support to the project pilots and integrators of the interoperability enablers (T5.5).

This WP is responsible for delivering InterConnect Interoperability Framework as a set of software tools and enablers for facilitating semantic interoperability between digital platforms, services and devices comprising the project pilots. The Interoperability Framework toolset is 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 work 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 in pilots with community-based use cases.

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, WP5 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 (SHBERA). All ontology and semantic interoperability specifications and requirements for the IC Interoperability Framework are provided by WP2.
- 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 specification of the DSO interface while WP5 provides integration of the service behind this interface with the Interoperability Framework and interoperable ecosystems established within the pilots.
- WP5 will provide WP7 pilots with the Interoperability Framework toolset as key input for realizing the project use cases leveraging established semantically interoperable ecosystems.

The WP7 pilots will provide continuous feedback leading to further updates of the Interoperability Framework.

- WP5 will provide cascade funding projects/partners (WP8) with the toolbox necessary for making their platforms and services interoperable with the Interoperability Framework and established pilots.

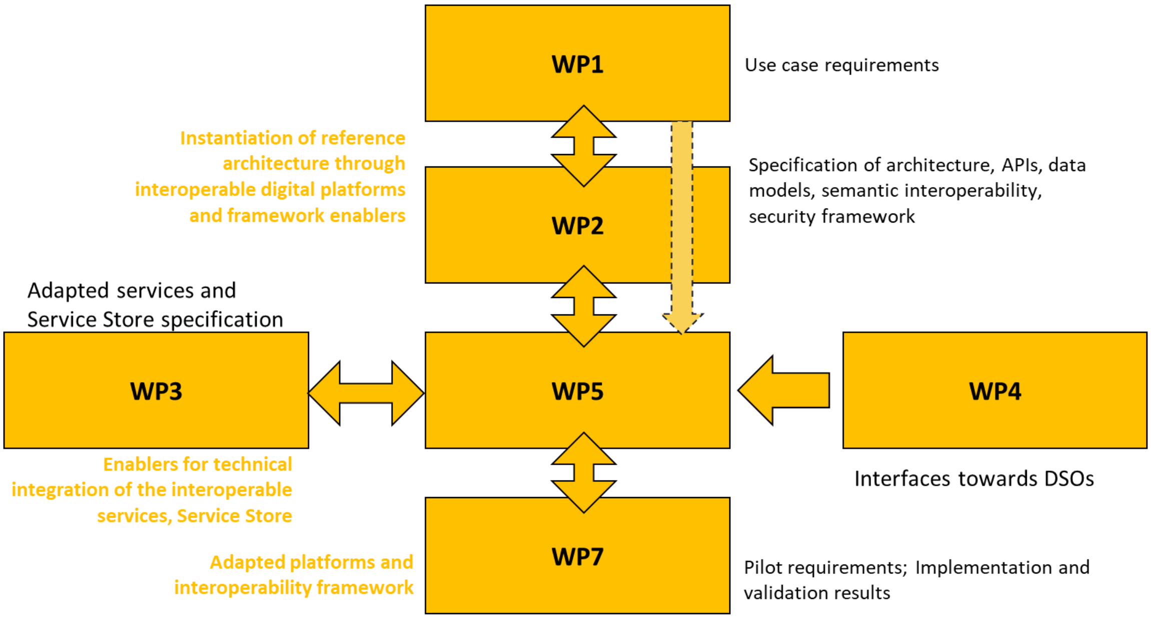
WP1
Use case requirements
Instantiation of reference architecture through interoperable digital platforms and framework enablers
WP2
Specification of architecture, APIs, data models, semantic interoperability, security framework
Adapted services and Service Store specification
WP3
WP5
WP4
Enablers for technical integration of the interoperable services, Service Store
Interfaces towards DSOs
Adapted platforms and interoperability framework
WP7
Pilot requirements; Implementation and validation results

FIGURE 1 - RELATION OF WP5 TO OTHER WPS (ORANGE FONT MARKS INPUT FROM WP5 TO OTHER WPS)

1.3 D5.1 OBJECTIVES AND APPROACH

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:

- Conduct in depth analysis of the current landscape of projects and initiatives tackling the challenges of semantic interoperability – identify best practices and lessons learned that can benefit the InterConnect Interoperability Framework;
- Carry out a detailed analysis of the project’s digital platforms and services and their interoperability capabilities and requirements;
- Specify architecture of the Interconnect’s Interoperability Framework and its main components;
- Provide an initial overview of each (sub-)pilot’s interoperability requirements.

To produce the specification and architecture of the Interoperability Framework and define key components of the toolset, the WP5/T5.1 team applied a combination of top-down and bottom-up approaches. Top-down approach started with the analysis of other research projects and initiatives tackling the challenges of (semantic) interoperability. Specific focus was put on analysing lessons learned from the **European IoT Platform Initiative** projects: their experience in enabling semantic interoperability between IOT systems with centralized and distributed interoperability enablers and facilitators proved to be valuable input for drafting the Interoperability Framework concept. Next, **standard reference architectures for IoT and energy domains** were analysed with the goal of identifying necessary technology bridges for enabling intra and inter domain interoperability while ensuring that reference architectures can be mapped onto interoperable ecosystems.

The bottom-up approach started with compiling the InterConnect catalogue of digital platforms provided by the consortium members. A template was provided to all digital platform providers so that capabilities and requirements of these platforms are documented in uniform format as to enable a comprehensive analysis. After the catalogue was compiled, WP5 proceeded with **analysis of the digital platforms provided by the project partners** which have to be made semantically interoperable in order to be used as a basis for building interoperable ecosystems represented by the project pilots. Interfacing capabilities are assessed in detail so that we can ensure that proposed interoperability enablers can in fact be employed by platform operators without disrupting already established processes and business logic. Finally, we have analysed **interoperability requirements of all project pilots** to identify interoperability points to be established between participating digital systems and assess requirements for facilitating these interoperability points.

In parallel with this process, the project level work on InterConnect reference architecture, semantic interoperability specification and ontology development is followed during Interoperability Framework architecture drafting.

Based on analysis results and inputs from all these steps and approaches, WP5 produced the specification of the Interoperability Framework architecture. The architecture identified 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. The complete process followed by the WP5 towards specification, and further implementation, of the InterConnect Interoperability Framework is depicted in Figure 2.

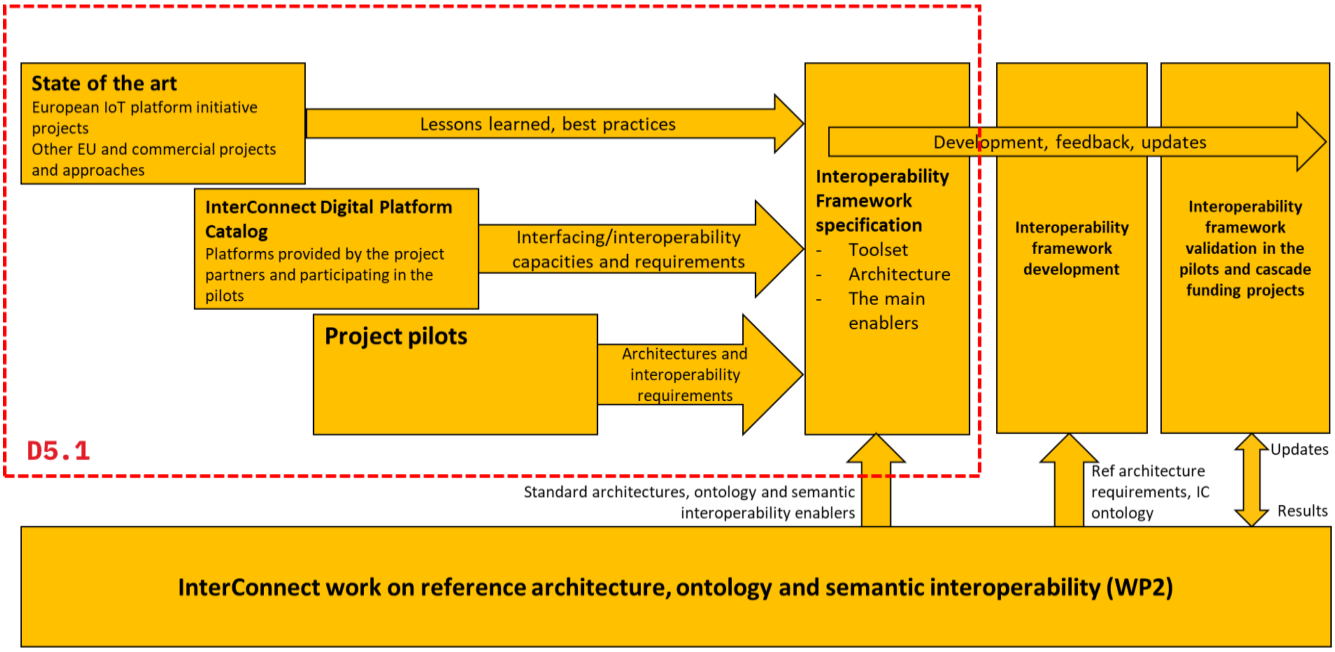
State of the art
European IoT platform initiative projects
Other EU and commercial projects and approaches
Lessons learned, best practices
InterConnect Digital Platform Catalog
Platforms provided by the project partners and participating in the pilots
Interfacing/interoperability capacities and requirements
Project pilots
Architectures and interoperability requirements
D5.1
Interoperability Framework specification
- Toolset
- Architecture
- The main enablers
Development, feedback, updates
Interoperability framework development
Interoperability framework validation in the pilots and cascade funding projects
Standard architectures, ontology and semantic interoperability enablers
Ref architecture requirements, IC ontology
Updates
Results
InterConnect work on reference architecture, ontology and semantic interoperability (WP2)

FIGURE 2 - APPROACH APPLIED BY WP5 TOWARDS SPECIFICATION OF THE INTEROPERABILITY FRAMEWORK ARCHITECTURE

The Interoperability Framework provides universal approach for enabling the syntactic and semantic interoperability needed for establishing semantically interoperable ecosystems that represent project pilots. The framework is not specifically tailored to address only the project pilots, but it is flexible enough to allow establishing new semantically interoperable ecosystems and combining ecosystems into more pervasive interoperable federations. The enablers specified in this document considered the existing technological requirements and limitations of digital platforms and services provided by the project partners to ensure technology uptake and its exploitation outside of the scope of the project as well. The approach is not disrupting the interfaces and business logic of the high TRL solution operated by the pilot stakeholders but **enables them to achieve semantic interoperability while respecting and supporting maintenance of established operational procedures**.

The framework enables the establishment of semantically interoperable ecosystems with federated knowledge pools (see Figure 3 for illustration). On top of these ecosystems, innovative services and applications can be built leveraging the established federated knowledge bases. Finally, the innovative services capable of utilizing federated knowledge across different digital systems and domains, motivate decision makers to pursue business level interoperability which directly impacts the market and provide new added values to the end users and to the businesses themselves.

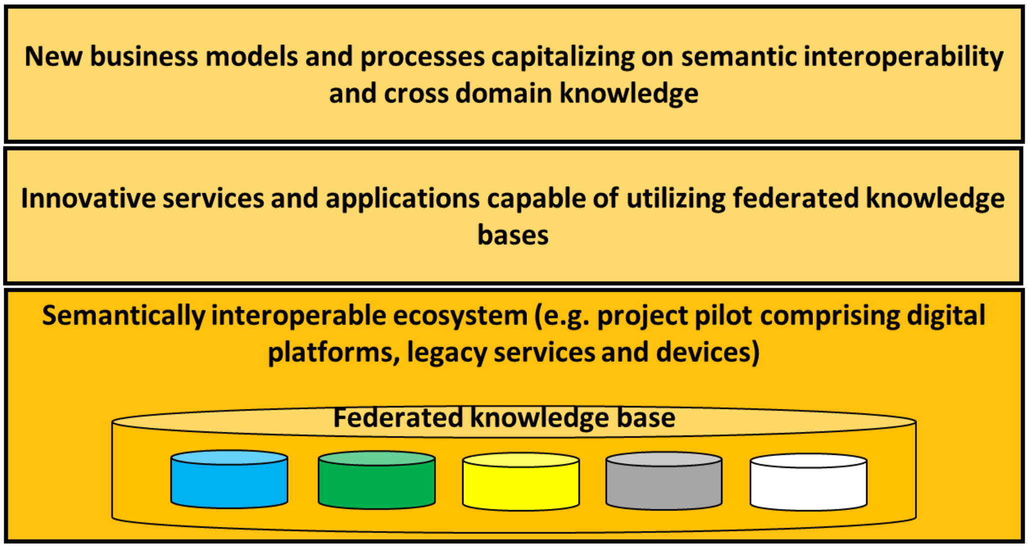
New business models and processes capitalizing on semantic interoperability and cross domain knowledge
Innovative services and applications capable of utilizing federated knowledge bases
Semantically interoperable ecosystem (e.g. project pilot comprising digital platforms, legacy services and devices)
Federated knowledge base

FIGURE 3 - SIDE VIEW SHOWING HOW NEW APPLICATIONS AND BUSINESS MODELS ARE BUILT ON TOP OF THE SEMANTICALLY INTEROPERABLE ECOSYSTEM ENABLED WITH THE INTEROPERABILITY FRAMEWORK

1.4 DOCUMENT STRUCTURE

This introduction is part of **Chapter 1**. It is followed by the table of common definitions used within this document and other technical and non-technical deliverables published by the InterConnect project. The overall organization of the chapters follows the WP5 methodology presented in Figure 2.

Chapter 2 - State of the Art collects and analyses key concepts of other European initiatives focused on creating an interoperable ecosystem. Key takeaways from each reference projects are described. It concludes by offering a synthetic view of each project's key features and compares them to the InterConnect Interoperability Framework approach. The goal is to showcase that the Interoperability Framework continues the good work of previous projects and pushes it forward into cross domain semantic interoperability enablement.

Chapter 3 - Interoperability of platforms, analyses the outcome of an internal survey carried out by WP5, cataloguing the available digital platforms (brought to the project by participating partners and their services), main functionalities, and their need (or not) for external services for supporting the SAREF ontology[3]. It concludes by discussing the interoperability requirements for supporting ICT technologies and the availability of interfaces deployment capabilities for virtual and scalable environments.

Chapter 4 - InterConnect Interoperability Framework Architecture introduces the tools and services that will enable existing digital platforms operated by the consortium partners to achieve

[3] The detailed results of this survey are presented in Annex 1 – Digital Platform catalogue.

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. The chapter provides high level definition of the methodology for building semantically interoperable ecosystem with the help of the Interoperability Framework.

Chapter 5 - Pilot's interoperability requirements and implementations strategy provide a quick overview of the mappings of the pilot's ecosystems onto the Interoperability Framework. Its placement on this document reflects the need for the reader to become familiar with the framework capabilities before being introduced with the complex ecosystems that are InterConnect pilots.

Finally, the document includes a set of concluding remarks in **Chapter 6** and **three Annexes** with detailed information on the catalogued digital platforms, specification and requirements of the project pilots and more details on the reference projects and initiatives.

2. STATE OF THE ART

This section provides 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. The goal was to identify best practices and success stories for these projects and use them as key inputs in the process of specifying the InterConnect Interoperability Framework architecture. Software artefacts from these projects are not directly used in the Interoperability Framework developments, but rather concepts and approaches for solving common challenges are taken and applied on the framework toolbox. **The goal of the InterConnect Interoperability Framework is to build upon the foundations set by previous projects and progress towards cross domain semantic interoperability enablers that will be validated in large scale pilots and improve overall update of the semantic web technologies in industry.**

Finally, this section offers a synthetic view of each projects' key features and compare it to those offered by the InterConnect Interoperability Framework. More details about these reference projects can be found in Annex 3 – State of the art: complementary information, of this document.

2.1 SYMBIOTE

The symbIoTe initiative (symbioses of smart objects across IoT environments) is an EU H2020 funded project. It provides a middleware framework covering all seven layers of the IoT World Forum' IoT Architecture[4]. The goal is to facilitate the creation of an interoperable IoT ecosystem, allowing for cross-platform interaction and the development of new domain-specific applications. A summary of key features is described as:

- Existing IoT platforms and services can use symbIoTe's Core Services to register and discover other functions.
- symbIoTe provides a flexible and incremental approach to interoperability, ranging from purely syntactic and semantic to full ecosystems where smart objects can interact.
- symbIoTe's Information Model provides a minimalistic but flexible core information model (CIM), promoting widespread platform adoption. However, it requires the definition of domain-specific extensions and mappings that need to be understood and agreed upon by various platforms when working with complex scenarios.
- symbIoTe offers a flexible and incremental approach to interoperability, introducing four compliance levels (CLs)

SymbIoTe addresses interoperability by considering a mapping approach where a custom data model is mapped into an interoperable one.

InterConnect leverages on this approach but extends it towards SAREF, also adopting the concept for interoperability compliance levels. InterConnect adopts a strategy based on SAREF ontologies for data exchange while not considering a central platform as data broker between entities.

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

2.2 BIG IOT

The BIG IoT (Bridging the Interoperability Gap of the Internet of Things) is an EU H2020 funded project. It focuses on the upper layers of the IoT architecture, through its API for resource sharing and discovery. The 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. A summary of key features is described as:

- BIG IoT offers a Marketplace with additional resources to expand the project's ecosystem. 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.).
- The project offers four different implementation modes [1], following the identification of five types of IoT platforms available within the project and their technical specificities (e.g., infrastructure, computational capacity, availability of the resources, etc.)
- Semantic and syntactic interoperability is achieved via the definition of a core model, extended with domain-independent and domain-specific vocabularies. BIG IoT's Semantic Reasoner also allows for data inference made available via SPARQL.

InterConnect's logical architecture leverages from BIG IoT's, establishing local services that attach to digital platforms, while not requiring a central platform as broker. Both initiatives employ a semantic reasoner for enriched data inference, being InterConnect's tailored for SAREF ontologies, providing coverage to energy and IoT domains. InterConnect also leverages from the service marketplace/store concept, extending it for energy and non-energy service types.

2.3 INTER-IOT

INTER-IoT is an EU H2020 funded project. It focuses on six layers of the IoT Architecture, covering aspects ranging from physical components, network connectivity to QoS, and resource catalogue for service registering and discovery. The goal is to provide seamless interworking between heterogeneous devices, services, applications, and IoT platforms. A summary of key features is described as:

- INTER-IoT concept for Interoperability is achieved by translating each IoT platform's resources to INTER-IoT's common ontology model and its extensions, namely via W3C's core ontology SOSA.
- INTER-IoT provided a semantic middleware, enabling southbound device interfaces to exchange information that is stored in an RDF triple store and queried via SPARQL.

INTER-IoT builds semantic data exchange by adopting proprietary ontologies to a common one considered by this initiative, while focusing in the IoT realm of applications.

InterConnect leverages from INTER-IoT translation approach for interoperability, considering it for SAREF as its core ontology and adopting the same strategy for both energy and non-energy services.

2.4 SYNCHRONICITY

SynchroniCity is an EU-funded project developed within the H2020 initiative. Focusing on the upper layers of the IoT architecture, it offers a rich catalogue of services and functions via its IoT Data Market Place and compliable Smart City applications and services. A summary of key features is described as:

- SynchroniCity's data model is based on the Open & Agile Smart Cities (OASC) reference information meta-model and its extensions, namely NGSI data modelling.
- SynchroniCity's focuses on capturing IoT device's data and mapping properties for northbound use by applications found in its IoT data marketplace.

InterConnect leverages from the marketplace concept of SynchroniCity, extending it to the concept of interoperable services. The interoperability concept of InterConnect builds on top the syntactical interoperability capabilities of SynchroniCity achieved via its NGSI data modelling and provides the means for semantic interoperability, namely via the use of SAREF ontology.

2.5 VICINITY

VICINITY is an EU H2020 funded project. It addresses the five upper layers of the IoT Architecture and builds around the concept of "virtual neighbourhoods" to achieve interoperability across distributed (i.e., P2P) IoT ecosystems. A summary of key features is described as:

- VICINITY's provides semantic and syntactic interoperability 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.
- VICINITY realizes the concept of software adapter that enables VICINITY services to reach for VICINITY cloud providing capabilities such as discovery, semantic search and the provision of user notifications.

InterConnect leverages from the VICINITY's adapter concept to introduce the InterConnect's generic adapter as the key components for interconnecting interoperable systems on syntactic and semantic levels. InterConnect's generic adapters are part of a distributed setup that act as gateways towards the distributed semantic interoperability layer for data exchange. Moreover, the concept for sematic data realization is also considered, being for InterConnect focused on SAREF.

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. It focuses on six layers of the IoT Architecture and aims to produce an experimental blueprint containing tools, techniques, and best practices for large scale deployments for distributed (geographically and administratively) IoT platforms. A summary of key features is described as:

- FIESTA-IoT focuses on the conceptualization of a single ontology, built from already existing multi-domain ontologies, with the aim to unify IoT control.
- FIESTA-IoT considers three different viewpoints for describing its IoT Reference Architecture, i.e., the information, deployment, and functional views.

- The project's core ontology model supports spatial queries and data inference (e.g., mobility of resources) via SPARQL queries.

InterConnect also considers the concept of ontology-centric developments as did FIESTA-IoT project. InterConnect also aims at extensibility of the Interoperability Framework by making it ontology agnostic. The semantic interoperability layer is based on SAREF family of ontologies, but it can be extended with additional ontologies for different pilots. The goal of InterConnect is to bring the semantic web technology closer to digital system operators by not disrupting their interfacing capabilities and approaches.

2.7 AGILE IOT

The AGILE (Adaptative Gateways for dIverse muLtiple Environments) project is co-founded by the H2020 EU program under the European IoT Platform Initiative. Its goal is to provide a flexible hardware and software gateways for building IoT solutions that enable seamless and modular integration of various devices. A summary of key features is described as:

- 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[5].
- AGILE IoT does not define an approach for semantic interoperability.
- Provides tools for easy roll-out of IoT gateways and associated data management,

While AGILE IOT does not cater for semantic interoperability, it provides the groundwork in the conception of a framework to enable an easy implementation of IoT gateways.

InterConnect leverages from this concept and translates it into the Interoperability Framework as a set of tools to enable seamless semantic interoperability and semantic data exchange. The goal of the Interoperability Framework is to support deployment of semantic interoperability enablers on all system levels from devices towards the cloud. Therefore, AGILE IoT gateway framework is important reference for building gateway/edge deployment options for the Interoperability Framework. Finally, the AGILE cybersecurity, attribute-based access control and identity management approach is used as the basis for InterConnect’s Service Store identity management and access control framework.

2.8 BIOTOPE

bIoTope is an H2020 EU funded project. It follows a system-of-system approach for building an open, interoperable ecosystem, allowing for rapid use case implementation. Its goal is to offer the necessary APIs that can help enable horizontal interoperability across cross-domain silos. A summary of key features is described as:

- bIoTope's architectural framework is built around a set of scalable micro-services, with data wrappers to accommodate integration with services and/or devices.
- 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.

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

- Provides a service catalogue / marketplace for service discovery and semantic data exchange.
- Provides security and privacy capabilities embedded into the micro-services made available.

InterConnect adopts the system-of-systems approach represented in bIoTope. This allows to compose several complex services by relying in simpler, interoperable and SAREF enabled services. As services are exposed via scalable micro-services, the use of data wrappers also contributes to the system-of-systems approach, which InterConnect also includes. Finally, the system-of-systems concept is used to guide specification of security and privacy protection plans of all project pilots and the Interoperability Framework.

2.9 ANALYSIS AND COMPARISON

This section summarizes the key concepts and functionalities provided by previous initiatives and shows how InterConnect leverages its work, or how it departs from them based on lessons learned and project specific requirements. To provide a synthetic, yet comparable view on all projects, the following categories are considered:

- **Domain,** providing an overview of the key sectors or domains in which the initiative is involved.
- **Marketplace**, regrouping three sub-categories detailing the main functions offered by each project's marketplace, namely:
  - **Metadata, annotations**, covering the exchange of interoperable metadata and annotations on a cross-platform or cross-domain setting amongst stakeholders.
  - **Registry & Discovery,** regrouping initiatives offering the possibility to Register and Discover new services via the project's marketplace.
  - **User Interface**, regrouping projects where a Graphical User Interface (GUI) facilitates a common user interaction with the project's marketplace (e.g., registering a device).
- **Interoperability Framework**, providing 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, overviewing the architectural layers covered by each project's reference framework[6].
  - The **Information Model**, describing each project's approach to semantic and syntactic interoperability. Four distinct cases were 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 interoperability amongst stakeholders.
  - The **Semantic Reasoner**, regrouping projects where semantic reasoning capabilities were included, i.e., new data can be inferred from existing knowledge.

[6] There are seven levels: 1. Physical Devices or "Things", 2. Connectivity, 3. Edge Computing, 4. Data Accumulation, 5. Data Abstraction, 6. Application Layer, and 7. Collaboration and Processes. These layers were described at the beginning of this section. For a more detailed description, visit: http://cdn.iotwf.com/resources/72/IoT_Reference_Model_04_June_2014.pdf

Table 1 summarizes and classifies key features.

		Marketplace			Interoperability Framework		
	Domain	Metadata, annotations	Registry & Discovery	User-Interface	Interoperability 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	✓	✓	✓	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, B, M	✓	✓	✓	1-7	E+X	✓

TABLE 1 – ANALYSIS AND COMPARISON OF KEY FEATURES ACROSS PROJECTS

Label

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

The analysed initiatives/projects provide a common ground of required capabilities which InterConnect requires, leveraging from conceptual outputs and approaches of the surveyed initiatives. This does not preclude the use of the tools themselves, but rather the concepts that will be latter on integrated in InterConnect's approach towards interoperability.

From the ongoing analysis, InterConnect realizes the need for several key concepts, namely:

- Semantic interoperability for seamless data exchange facilitated in distributed manner without centralized facilitator;
- Reasoning for data inference and discovery paving the way for cross domain federated knowledge bases;
- Reach for cross-domain (beyond IoT) data mappings;
- Ontology scalability and cross-domain mapping capability;
- Scalable and flexible deployment capabilities, via the system-of-systems concept;
- Security and data privacy intertwined with the semantic interoperability processes.

3. INTEROPERABILITY OF DIGITAL PLATFORMS

InterConnect brings together key stakeholders from the IoT and energy domains. They bring to the project digital platforms which are used in their service offerings and system integrations.

WP5 produced detailed catalogue of all digital platforms provided by the project partners for execution of the project pilots. All platform operators are provided with the same template for describing key capabilities of their digital solutions including interfacing capabilities, interoperability potential (using standard protocols, data formats, data models and ontologies), provided energy and non-energy services and security and privacy protection capabilities. Having all information provided in uniform format allowed us to perform in depth analysis of the digital platforms' capabilities and requirements for achieving semantic interoperability aimed by the project pilots. This insight was one of the key inputs into the process of specification of the Interoperability Framework. The key inputs from the digital platform catalogue are provided in the Annex 1 of this document.

The main milestone and KPI to be achieved on behalf of WP5 is the provision of semantic interoperability between digital platforms and services within the same domain and across domains. This 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*** **–** they provide means for domain and operational data sharing between stakeholders. Since the set of available digital platforms in this project exposes a wide and complex set of services and interfacing capabilities, it should be noted that many of them **do not include**, at this stage, **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 semantically interoperable way. This implies that for the most digital platforms and their services there is the need to undergo a ***SAREFization process*** (detailed in 3.3.1) that accommodates the data identification, translation, and technical integration with InterConnect's semantic interoperability layer.

The following sub-sections summarise the main findings of an internal survey that identified 25 digital platforms and highlights their general architectures and interoperability indicators[7].

The adoption of ontologies is also covered in this section, particularly the ones within the SAREF ecosystem, and the need for external services. Finally, it 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 cloud infrastructures.

3.1 DIGITAL PLATFORMS OVERVIEW

The results of the survey can be interpreted following a taxonomy composed of ten key 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 the focus of any 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; **Smart Buildings** to identify platforms and services that address connectivity to/from/within smart buildings; **IoT** to identify platforms and services that act as software gateways to handle devices and

[7] The detailed results of this survey are featured in Annex 1 – Digital Platform catalogue.

feature across specific domains; **Energy** to identify platforms or services that address specific needs for energy, grid management or that induce energy savings and overall grid management.

Type. This property characterises the focus for most functions and services made available by any 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 knowledge; **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.

Table 2 overviews the digital platforms addressed during the survey of InterConnect digital platforms, classifying them according to the considered taxonomy.

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, ED, C	↑⌬↓	Y	N, A	JSON	Y	Y
EBO	Schneider 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
Cognitive Load	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

3.1.1 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 semantic interoperability layer, this section will analyse the capabilities of available services provided by the digital platforms.

Domain and advanced services comprehend the functionalities that are related with the domains identified within InterConnect, namely the Energy, IoT and Smart Homes/Buildings. These domains were chosen as they represent most 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 [11]. Moreover, the Interoperable 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	Schneider 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 DOMAIN AND ADVANCED SERVICES

3.1.2 INTERFACES AND SUPPORTING TECHNOLOGIES

This section overviews the interfaces made available by 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 4 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	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	TNO	✓						✓				✓		✓
ThermoVault	ThermoVault		✓								✓			
Sensinov	Sensinov	✓		✓	✓		✓	✓		✓	✓	✓		
EBO	Schneider 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 OF AVAILABLE INTERFACES BASED ON THE DIGITAL PLATFORM CATALOGUE

3.2 DISCUSSION OF THE DIGITAL PLATFORM CATALOGUE

The provided digital platforms offer different services towards IoT, smart homes, smart buildings, and the grid. Each one of these domains implies distinct interaction patterns that are relevant to highlight.

IoT and energy centric digital platforms imply the use of particular standards, data formats and consequently distinct interfacing technologies. While it is natural to assume that each domain (i.e., IoT and an Energy) imposes restrictions and even conventions that are used within, doing so impairs interoperability and, most importantly, impairs a common understanding on what data means and how it is applied.

The lack of truly interoperable solutions found in this ecosystem is mainly justified by that fact that there is no shared concept of the data interpretation and knowledge representation. Hence, InterConnect proposes the adoption of semantic driven data exchange, where the meaning of data (domain specific included) is unbiasedly specified by means of the SAREF ontology.

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 [12], twenty-three digital platforms are currently at a SAREF compliance level 0 (*i.e., no SAREF compliance on data, metadata, or reasoning*).

This approach systematically provides a way for data to be expressed in the scope of the domain it represents and, most importantly, enables other entities (outside the origin domain) to have full grasp on data meaning (i.e., representativeness, units of measure, applicability, etc).

The interoperability impairment then arrives at the technical level, where several transmission technologies can be employed to transmit “the” common understanding.

While InterConnect does not cater for all possible transmission protocols, it takes them into consideration, and adopts REST-full web-services as the transmission protocol due to its representativeness in our consortium, but also, outside of it.

At the same time, is not possible to admit that all platforms and services would undergo a massive redesign, hence impairing services already deployed in practice. Therefore, InterConnect considers a **wrapper** approach by employing the InterConnect adapter and providing means for interoperability but leaving at the discretion of digital platform or service owners the decision on how, and to what extent they want to make their platforms interoperable.

Thus, adopting the interoperable solution proposed by InterConnect comes down to undergo a systematic process, which the consortium designates as “*SAREFization”* to perform data mappings, derive data relationships and accommodate technical integration. Ultimately, this will unlock interoperability for domain specific services and digital platforms.

3.3 INTEROPERABILITY REQUIREMENTS

The previous sub-sections identify and characterize the available digital platforms, according to several axis, namely: the overall positioning (Table 2), the domain and services (Table 3) and the supporting technologies and interfaces (Table 4).

To support the discussion regarding interoperability requirements, Figure 4 depicts a preliminary view regarding the interoperability layer to be introduced in Section 4 of this deliverable.

To support the provision of interoperability, several tools are required to enable semantic data exchange, and to support operation, making the available set of service and capabilities visible. This section drafts the vision and details the requirements for interoperability according to InterConnect Interoperability Framework concept.

The provision of interoperability is based on the concept of "*Adapters"* that allow the necessary adjustments and become the gateway 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 based on the underlying native technologies for transport and execution.

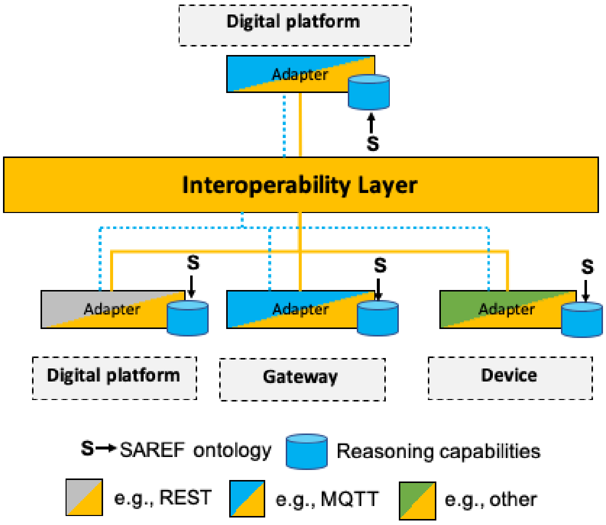

FIGURE 4 - PRELIMINARY ENTITY MAP FOR THE ARCHITECTURE

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**.

3.3.1 SEMANTIC AND REASONING REQUIREMENTS

Semantic reasoning will be the distinguishing capability for the provision of interoperability within InterConnect. Semantic reasoning is 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 able to express their features with the aid of ontologies, which for the case of InterConnect are the ones belonging to the SAREF family. With established semantic interoperability and deployed reasoning functionalities, federated knowledge bases can be established as the basis for building innovative cross domain services and new business models.

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 [12] (i.e., metadata and/or data use SAREF and reasoning is enabled) digital platforms will be required to undergo the *SAREFization* process, that summarizes as (see Figure 5):

1. Address service capabilities and matching them with SAREF descriptions;
2. Address service messages and units of measure and match them with SAREF descriptions;
3. Candidate graph patterns for services as ways to disseminate service messages and instructions through the semantically interoperable layer;
4. Technical integration with the Generic Adapter provided by the Interoperability Framework;

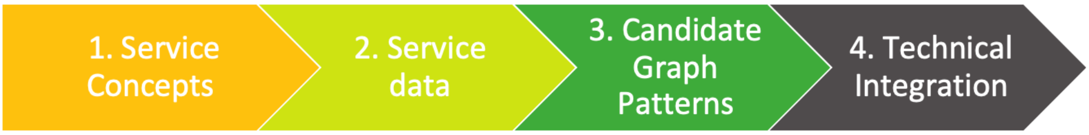

FIGURE 5 - SAREFIZATION PROCESS

3.3.2 INTERCONNECT GENERIC ADAPTER

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 [12], the adoption of an *"adapter"*, as a lightweight software package, will bring common data translations in a mesh of adapters building interoperable ecosystems.

Generic adapter must 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) and northbound interfaces (i.e., the interface exposing service/platform capabilities to the interoperable ecosystem).

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

- Accommodate the semantic and reasoning requirements described in section 3.3.1;
- Consider, if needed, any required adjustment to the service API;
- Undergo the SAREFization process;
- Undergo technical integration with the Generic Adapter;
- Consider the required data translation from the (southbound) digital platforms and services to be fed into InterConnect's Interoperability Framework.

The Interoperability Framework Generic Adapter is described in more details in the next section.

4. INTERCONNECT INTEROPERABILITY FRAMEWORK ARCHITECTURE

The InterConnect project seeks to achieve semantic interoperability between existing platforms, services and devices 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.

The InterConnect Interoperability Framework Architecture (IFA) is the result of a methodology taken by all stakeholders, briefly in the following steps (see Figure 2):

- Analysis of the key outputs of other project and initiatives tackling the challenge of interoperability.
- Analysis of reference architectures from standards and other initiatives, especially those from the IoT end energy domains.
- Analysis of consortium partners' digital platforms in terms of architectures, interfacing capabilities, services, and interoperability requirements.
- Collecting inputs and interoperability requirements from project pilots identifying integration points between participating digital systems.
- Alignment with WP2 work on InterConnect reference architecture, SAREF based ontology development and semantic interoperability approaches.
- SAREFization process for digital systems (platforms, services, and devices) is defined in cooperation with WP3.
- The process finished with design and technical specification of the components of the IFA.

The first output of the analysis process performed by the T5.1 was a set of requirements that the InterConnect Interoperability Framework must fulfil. Table 5 introduces the list of requirements that have impacted the specification and development of the InterConnect Interoperability Framework.

Requirement #	Requirement description
R1	IC project MUST achieve semantic interoperability without a centrally hosted digital platform to facilitate interoperability.
R2	IC project SHOULD achieve semantic interoperability based on SAREF ontology and a set of existing, already validated semantic reasoning and orchestration technologies. The project ontology SHOULD extend SAREF and also provide opportunity for integration of additional standard ontologies.
R3	IC project MUST specify the Interoperability Framework providing enablers and services for realization of interoperable environments required by the project pilots and defined use cases. The set of enablers MUST be minimally disruptive towards already existing interfacing technologies and service logics brough in by high TRL digital platform comprising the pilots.
R4	IC Interoperability Framework SHOULD support different deployment options on different system levels – edge, fog, cloud.
R5	IC project SHOULD enable interoperability not just within pilots, but among them in overarching use cases.
R6	IC project MUST support cascade funding partners and integrators to utilize the Interoperability Framework components to make their platforms and services interoperable thus joining existing or establishing new semantically interoperable ecosystems/pilots.

R7	IC project SHOULD implement mechanisms for interoperability compliance test and certification to boost overall trustworthiness within and among semantically interoperable ecosystems.
R8	IC project MUST ensure that achieved interoperability does not impact or limit the privacy protection regulations and mechanisms already implemented by participating entities.
R9	IC Interoperability Framework MUST support configurable cybersecurity and access control methods that allow integrators to achieve semantic interoperability without impacting already established business and service provision logic.
R10	IC Interoperability Framework MUST provide overall catalogue of all interoperable services and digital systems as a reference for integrators to be able to choose best interoperable systems to employ in their interoperable ecosystems.
R11	IC Interoperability Framework MUST support innovative P2P data exchange paradigms and marketplaces leveraging distributed ledger technologies.

TABLE 5 - HIGH LEVEL REQUIREMENTS FOR IC INTEROPERABILITY FRAMEWORK

Based on these high-level requirements, a first general concept of the Interoperability Framework is specified with the following key components (as shown in Figure 6):

- Secured and trusted semantic interoperability layer represented by a set of distributed integration enablers and semantic discovery and reasoning functionality.
- Overall registry or catalogue of all interoperable digital systems published and provided in a way that streamlines onboarding of new catalogue entries and allows browsing and comparing capabilities of the catalogues entries.
- Configurable cybersecurity framework which protects data exchange channels through the semantic interoperability layer and at the same time allows integrators to restrict semantic discovery and reasoning freedom to adhere to their business and service provision logic.
- A trusted entity for issuing interoperability compliance certificates indicating level of interoperability and options for integration into interoperable ecosystems.

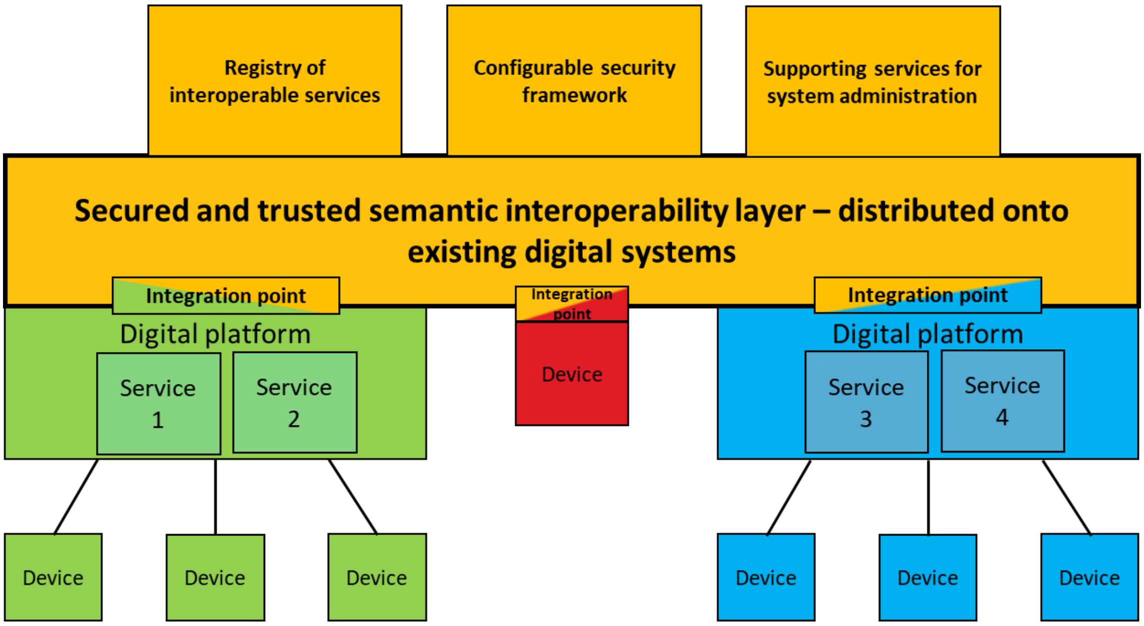
Registry of interoperable services
Configurable security framework
Supporting services for system administration
Secured and trusted semantic interoperability layer – distributed onto existing digital systems
Integration point
Integration point
Integration point
Digital platform
Service 1
Service 2
Device
Digital platform
Service 3
Service 4
Device
Device
Device
Device
Device
Device

FIGURE 6 – KEY SEMANTIC INTEROPERABILITY ENABLERS CAPABLE OF ADDRESSING THE REQUIREMENTS

This general Interoperability Framework represents a **set of tools and services which enable existing digital platforms, operated by the consortium partners, to achieve semantic interoperability without the need for intermediary platform dedicated to hosting interoperability adapters**. This set of key semantic interoperability enablers was used as high-level specification of the InterConnect Interoperability Framework and led towards detailed specification of key components of the framework architecture as presented in the next section. The InterConnect Interoperability Framework is conceptualized to enable digital platforms with standard, or custom architectures to interoperate with other platforms and get access to additional services necessary for implementing innovative use cases and applications.

Key objective behind the specification of the InterConnect Interoperability Framework architecture was to consider the IC reference architecture as specified in [12]. The secure and interoperable reference architecture for smart buildings and smart grids provides a tiered map, composed of several layers spanning from the more south-bound device layer, up until the north-bound application layer. The high-level architecture provides the needed merge between IoT with the Energy domain in a cohesive approach. This reference architecture provides the means to map digital platforms and services and highlight the need for interoperability. Some functional layers of the reference architecture are already represented in the digital platforms provided by the project partners. 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. The Interoperability Framework is conceptualized to enable the instantiation of the InterConnect reference architecture on digital platforms and other endpoints constituting the project pilots.

The realization of the Interoperability Framework concept is the joint result from WP2, WP3 and WP5. WP2 provides the reference architecture, together with data modelling based on SAREF. WP3 addresses all candidate digital services and provides the specific data mappings (i.e., Service Specific Adapters – see section 4.2) that allow services to encode data and its representation according to SAREF. WP5 provides the design and implementation for the tools that make the Interoperability Framework, that will enable semantic data exchange between services. Moreover, it also addresses the security and privacy protection needs to sustain the pilots. Figure 7 presents functional map of the Interoperability Framework. The main functionalities are divided into:

- Integration group – including all functionalities for integrating existing digital systems (platforms, services and devices) into secured and trusted semantically interoperable ecosystems.
- Operations group – including all functionalities for managing established semantically interoperable ecosystems.

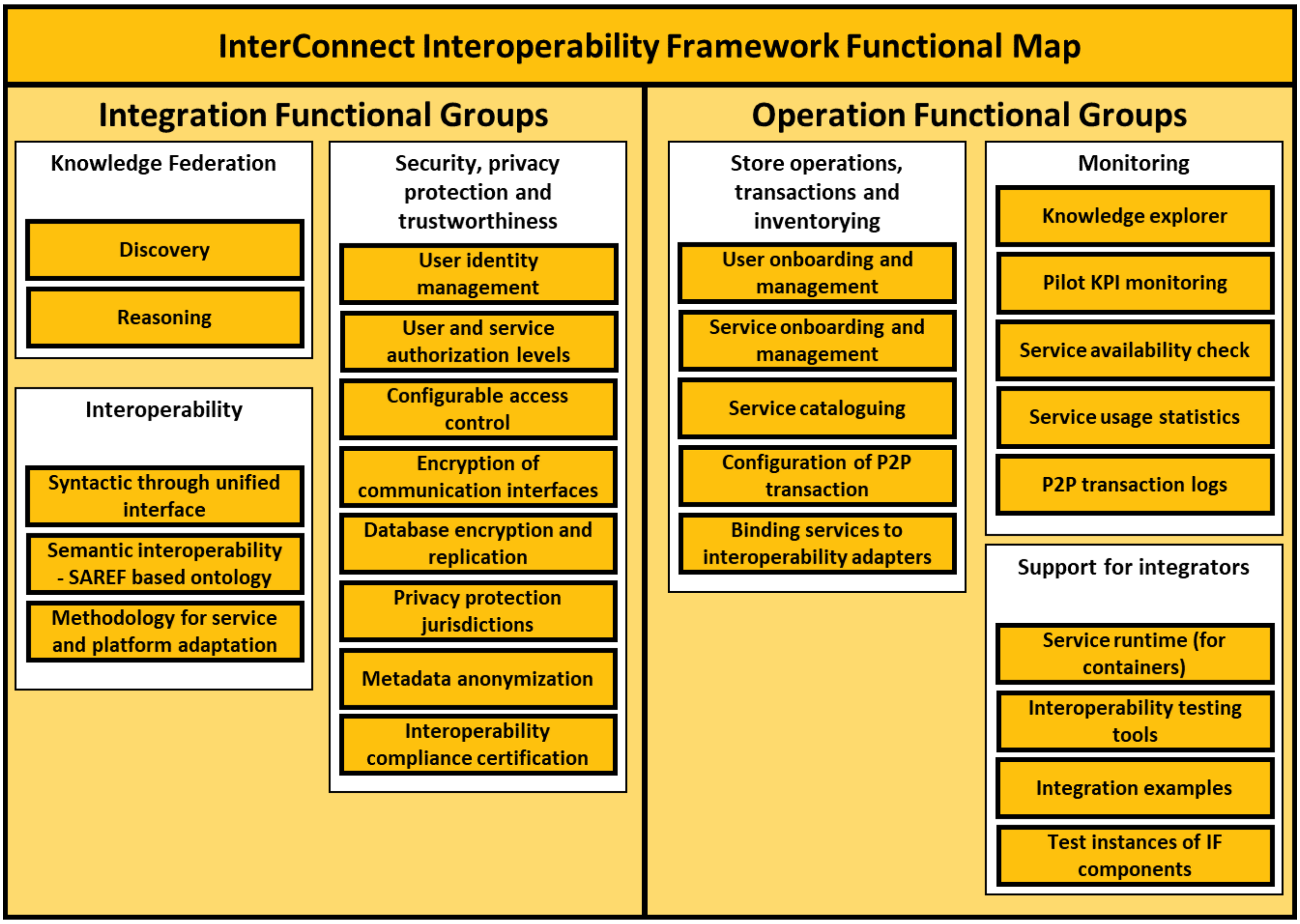
InterConnect Interoperability Framework Functional Map
Integration Functional Groups
Knowledge Federation
Discovery
Reasoning
Interoperability
Syntactic through unified interface
Semantic interoperability - SAREF based ontology
Methodology for service and platform adaptation
Security, privacy protection and trustworthiness
User identity management
User and service authorization levels
Configurable access control
Encryption of communication interfaces
Database encryption and replication
Privacy protection jurisdictions
Metadata anonymization
Interoperability compliance certification
Operation Functional Groups
Store operations, transactions and inventorying
User onboarding and management
Service onboarding and management
Service cataloguing
Configuration of P2P transaction
Binding services to interoperability adapters
Monitoring
Knowledge explorer
Pilot KPI monitoring
Service availability check
Service usage statistics
P2P transaction logs
Support for integrators
Service runtime (for containers)
Interoperability testing tools
Integration examples
Test instances of IF components

FIGURE 7 - INTERCONNECT INTEROPERABILITY FRAMEWORK - FUNCTIONAL MAP

4.1 HIGH LEVEL FUNCTIONAL ARCHITECTURE OF THE IC INTEROPERABILITY FRAMEWORK

Based on the analysis process depicted at the start of section 4, project team prepared high level functional architecture of the IC Interoperability Framework as shown in Figure 8. In this figure we depict the main components of the framework in a typical deployment scenario where two digital platforms from different stakeholders establish a semantically interoperable ecosystem. Available digital platforms will run interoperable energy and non-energy services necessary for the realization of pilot use cases. Therefore, most of the IC Interoperability Framework enablers are targeting digital platforms and services hosted on them. The key components of the framework are:

- The **Semantic interoperability layer** (addressing high level requirements R1, R2 and R4), which enables semantic interoperability and reasoning between all endpoints capable of running:
    - The **Generic adapter**, which provides orchestration and translation of existing interfaces and data models to the unified communication protocol and data model based on SAREF ontology.
    - The **IC interoperability connector**, which provides reasoning for endpoints which already expose an interface following unified communication protocol and data model based on SAREF ontology.

  - The semantic interoperability layer comprises configured instances of interoperability adapters and connectors (see Section 4.2.2) 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 5). The semantic reasoning and orchestration processes are also provided by the interoperability layer while the interoperable services are adapted to take full advantage of these semantic web mechanisms via SAREF.
- The **Security and data protection framework** (requirements R8 and R9 from Table 6), which is integrated with the Interoperability Framework so that defined access control and data/privacy protection rules, required by digital platforms and services.
- The **Service store** (requirement R10), providing the complete catalogue of interoperable services from energy and non-energy domains. The service store is implemented as a web application providing a frontend interface for onboarding and discovering services. The service store allows users or 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.
- **The P2P marketplace enablers** (requirement R11), which 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 the implementation of energy transactions as well as other data-related transactions common in community-based scenarios and use cases. The key components are:
  - Hyperledger Fabric configurations as a blockchain basis for trusted data access and transaction management.
  - Set of smart contract templates representing supported transactions, reports and integration points;
  - White labelled web application utilizing blockchain network through integrated smart contract interfaces.
- **Interoperability compliance tests and certificates** (requirements R7 from Table 6), a set of automated tests of achieved minimal interoperability defined for each service category. The interoperability compliance tests will be part of the service onboarding process in the service store. After a successful compliance test, a certification of interoperability compliance will be issued and written in immutable records of all interoperable endpoints based on Hyperledger Fabric blockchain established at the level of the IC project.
- **Supporting services** – a set of services and enablers that 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 the 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 R6 from Table 6).
  - Support for KPI collection at the Service Store level streamlining monitoring of the project use cases.

Each of these IC Interoperability Framework enablers and tools is introduced in greater detail in the following subsections.

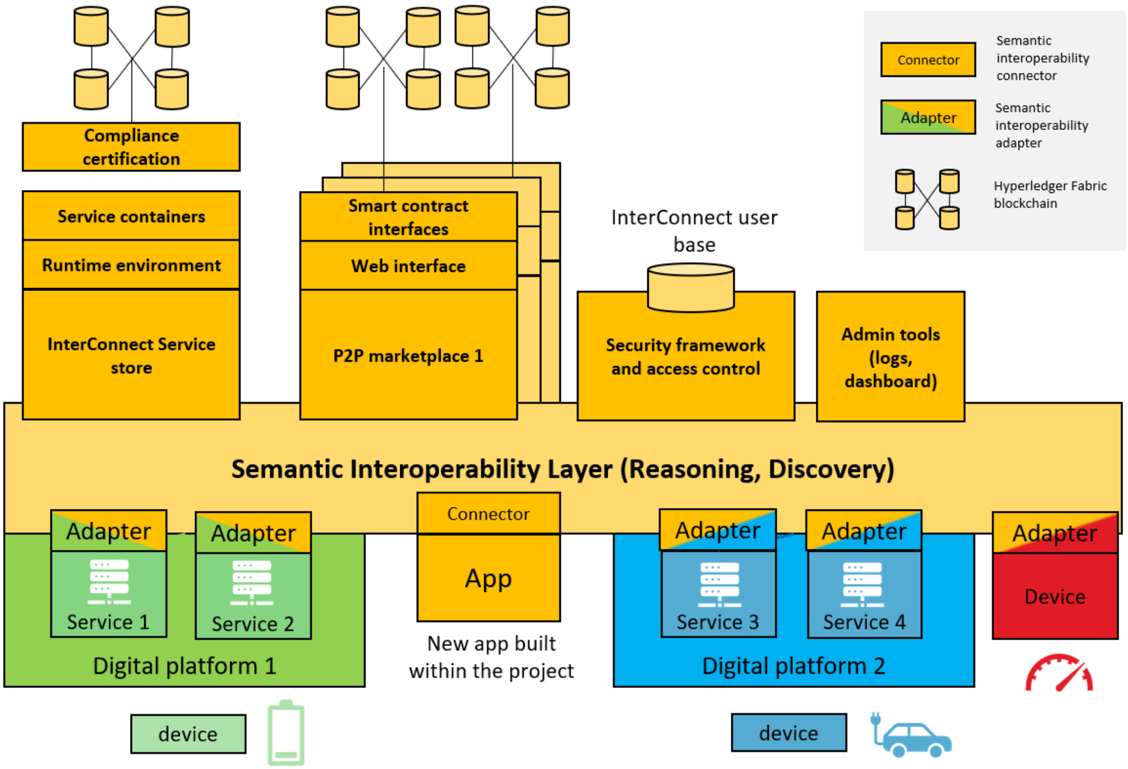
Connector
Semantic interoperability connector
Adapter
Semantic interoperability adapter
Hyperledger Fabric blockchain
Compliance certification
Service containers
Runtime environment
InterConnect Service store
Smart contract interfaces
Web interface
P2P marketplace 1
InterConnect user base
Security framework and access control
Admin tools (logs, dashboard)
Semantic Interoperability Layer (Reasoning, Discovery)
Adapter
Service 1
Adapter
Service 2
Digital platform 1
Connector
App
New app built within the project
Adapter
Service 3
Adapter
Service 4
Digital platform 2
Adapter
Device
device
device

FIGURE 8 - HIGH LEVEL FUNCTIONAL ARCHITECTURE OF THE IC INTEROPERABILITY FRAMEWORK

Each pilot will instantiate the specified InterConnect 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.

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 the latter, 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[8]. This means that interoperable services will be accessible and usable across and between pilots. Interoperable services supplied by the WP3, ontology supplied by the WP2, and interoperability framework supplied by the WP5 are the complete set of tools available for building semantically interoperable ecosystems (e.g. project pilots).

4.2 THE SEMANTIC INTEROPERABILITY LAYER

The Semantic Interoperability Layer (SIL) is the main component of the InterConnect Interoperability Framework. It is implemented as a distributed middleware responsible for facilitating secure and trusted semantic and syntactic interoperability between digital systems. In this subsection we will first discuss the concepts of interoperability, we will present InterConnect's approach for building a distributed middleware for semantic and syntactic interoperability, and, finally, we will present the specification of the main enabling components of the semantic interoperability layer.

[8] Specific approaches for distinguishing IC Interoperability Framework instances on pilot and project level will be specified within WP5 and T5.2.

4.2.1 CONCEPT OF SEMANTIC INTEROPERABILITY

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 to accurately reference the degree of interoperability. Figure 9 gives an overview of this framework (the GWAC stack).

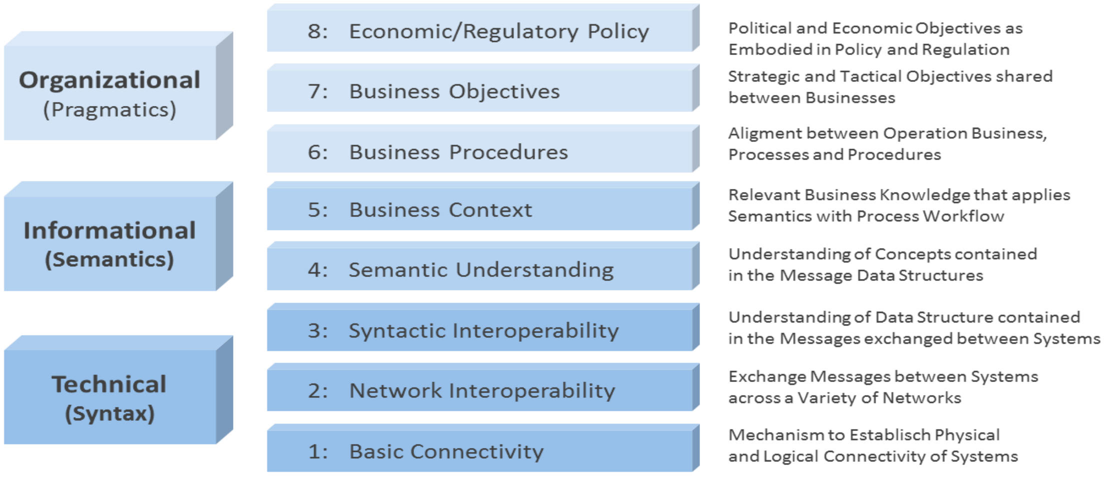
Organizational
(Pragmatics)
Informational
(Semantics)
Technical
(Syntax)
8: Economic/Regulatory Policy
7: Business Objectives
6: Business Procedures
5: Business Context
4: Semantic Understanding
3: Syntactic Interoperability
2: Network Interoperability
1: Basic Connectivity
Political and Economic Objectives as Embodied in Policy and Regulation
Strategic and Tactical Objectives shared between Businesses
Aligment between Operation Business, Processes and Procedures
Relevant Business Knowledge that applies Semantics with Process Workflow
Understanding of Concepts contained in the Message Data Structures
Understanding of Data Structure contained in the Messages exchanged between Systems
Exchange Messages between Systems across a Variety of Networks
Mechanism to Establisch Physical and Logical Connectivity of Systems

FIGURE 9 - LEVELS OF INTEROEPRABILITY (SOURCE GWAC - GRIDWISE ARCHITECTURE COUNCIL)

The sublevels: basic connectivity, network interoperability, syntactic interoperability, and semantic understanding are relevant for Smart Home systems. 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.
- **Network interoperability:** Network interoperability presupposes an agreement on how the information is transported between interacting parties across multiple communication networks.
- **Syntactic interoperability:** Technical interoperability guarantees the correct transmission of bits. Syntactic interoperability refers to the exchange of information between transacting parties based on agreed format and structure for encoding this information.
- **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).

The Interoperability Framework provides tools for facilitating syntactic and semantic interoperability between services.

4.2.2 INTERCONNECT'S APPROACH FOR BUILDING DISTRIBUTED MIDDLEWARE FOR SEMANTIC AND SYNTACTIC INTEROPERABILITY[9]

InterConnect's Semantic Interoperability Layer (SIL) 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**. This approach enables the creation of cross-domain federated knowledge bases among participating stakeholders and their interoperable digital systems.

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 (SAREF based data models). These enablers are the **Generic Adapter and the Interoperability Connector**.

The Generic Adapter (see Figure 10) is to be instantiated per endpoint (software service, digital platform, device) which needs to be made interoperable. The Generic Adapter provided by the Interoperability Framework can then be customized to specific service types via the Service Specific Adapters developed within WP3 (see Figure 11). This Service Specific Adapter is part of the SAREFization process for the services and it performs mapping of the service interface onto the unified interoperability interface and maps data models onto the SAREF ontology (more details provided in the next subsection). **Services equipped with this set of interoperability adapters do not need to know API specification of other interoperable services in order to communicate with them. They need to use/understand the same ontology.**

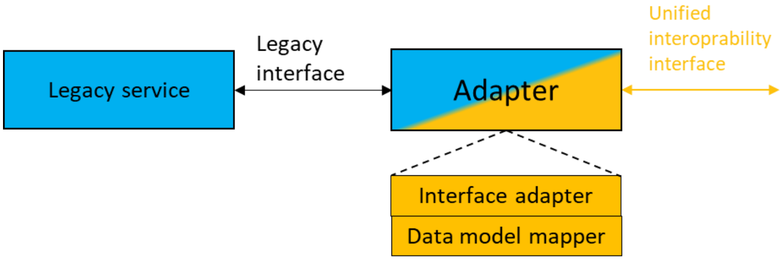

FIGURE 10 - HIGH LEVEL OVERVIEW OF THE INTEROPERABILITY ADAPTER

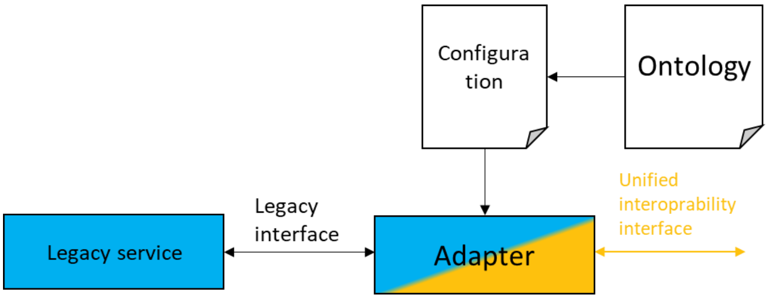

FIGURE 11 - HIGH LEVEL OVERVIEW OF THE IC INTEROPERABILITY ADAPTER WITH CUSTOM CONFIGURATION

The IC interoperability connector (see Figure 12) will enable application and services purposefully built for the IC project to utilize the semantic reasoning and orchestration functionalities provided by the IC

[9] Please note that in all subsequent figures and 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 legacy interface implementation.

semantic interoperability layer. The assumption is that applications and services developed during the project will utilize SAREF based data models and expose the interoperable interface.

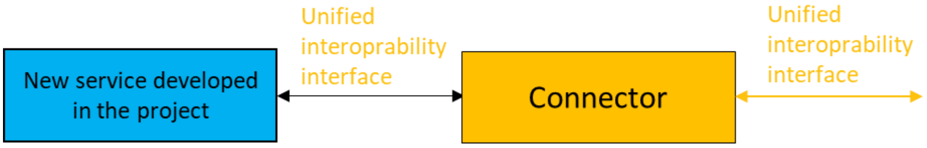
New service developed in the project
Unified interoprability interface
Connector
Unified interoprability interface

FIGURE 12 - HIGH LEVEL OVERVIEW OF THE IC SEMANTIC INTEROPERABILITY CONNECTOR

With the concept of Generic Adapter defined, the IC semantic interoperability layer can be presented in more details. Figure 13 shows a typical pilot ecosystem comprising two different digital platforms, each with its own set of services, managed devices and interfaces; a service running on a platform that might not be part of the InterConnect digital platform catalogue; an 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); and the IC Interoperability Framework, with specific focus on the IC semantic interoperability layer. The latter is showcased as a layer/architecture component responsible for bridging/interconnecting services, applications and platforms all utilizing different communication interface technologies/protocols/standards.

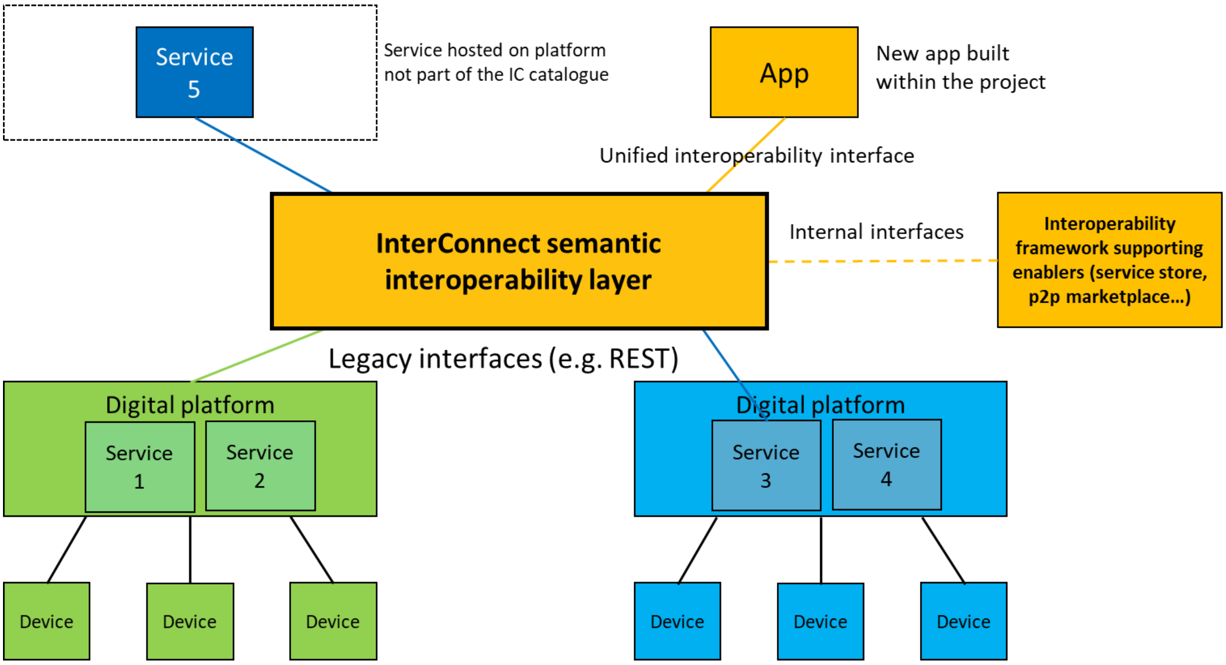
Service 5
Service hosted on platform not part of the IC catalogue
App
New app built within the project
Unified interoperability interface
InterConnect semantic interoperability layer
Internal interfaces
Interoperability framework supporting enablers (service store, p2p marketplace…)
Legacy interfaces (e.g. REST)
Digital platform
Service 1
Service 2
Digital platform
Service 3
Service 4
Device
Device
Device
Device
Device
Device

FIGURE 13 - SEMANTIC INTEROPERABILITY LAYER IN CONTEXT OF A TYPICAL PILOT ARCHITECTURE

Figure 14 showcases the components of 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.

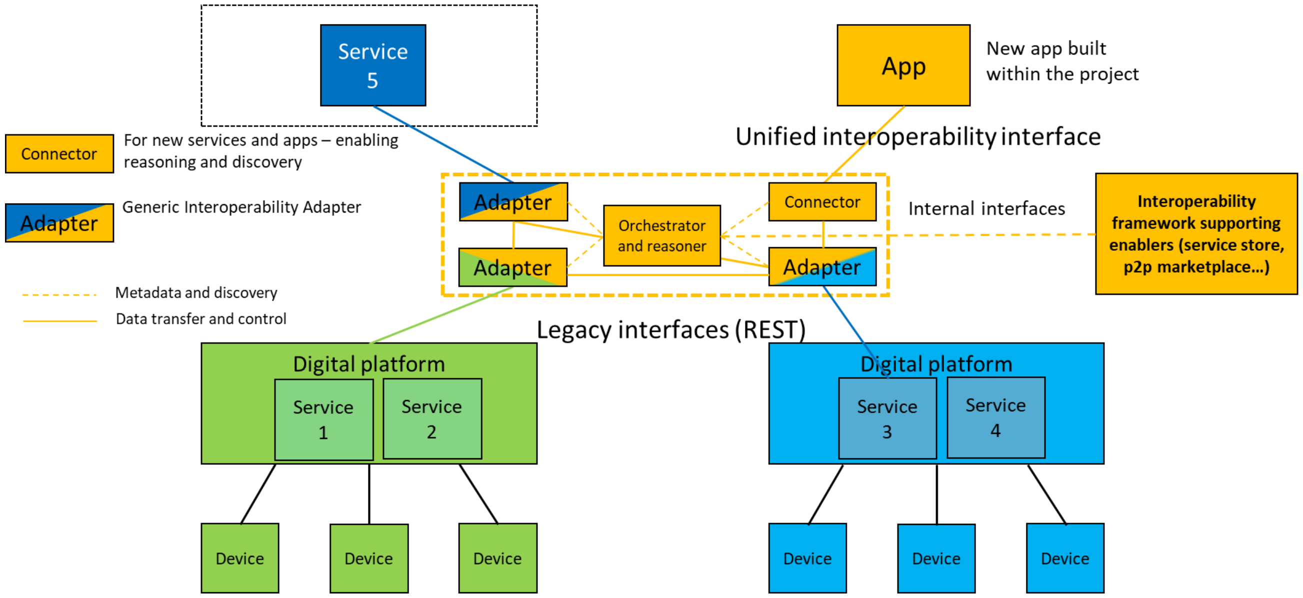
Service 5
App
New app built within the project
Connector
For new services and apps – enabling reasoning and discovery
Unified interoperability interface
Adapter
Generic Interoperability Adapter
Adapter
Orchestrator and reasoner
Connector
Internal interfaces
Interoperability framework supporting enablers (service store, p2p marketplace…)
Adapter
Adapter
Metadata and discovery
Data transfer and control
Legacy interfaces (REST)
Digital platform
Service 1
Service 2
Digital platform
Service 3
Service 4
Device
Device
Device
Device
Device
Device

FIGURE 14 - IC SEMANTIC INTEROPERABILITY LAYER COMPRISING GENERIC INTEROPERABILITY ADAPTERS

Figure 15 shows InterConnect's approach for deploying the IC interoperability layer. The goal is to distribute the IC interoperability adapters towards the endpoints which need to interoperate. 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. Therefore, the semantic interoperability can be enabled without a centrally hosted facilitator/platform. The Generic Adapter can be instantiated **on the level of a service** (each service with its own adapter), or **at the level of the whole digital platform** running multiple services. The approach on how to instantiate the adapters will be decided by the platform and service operators.

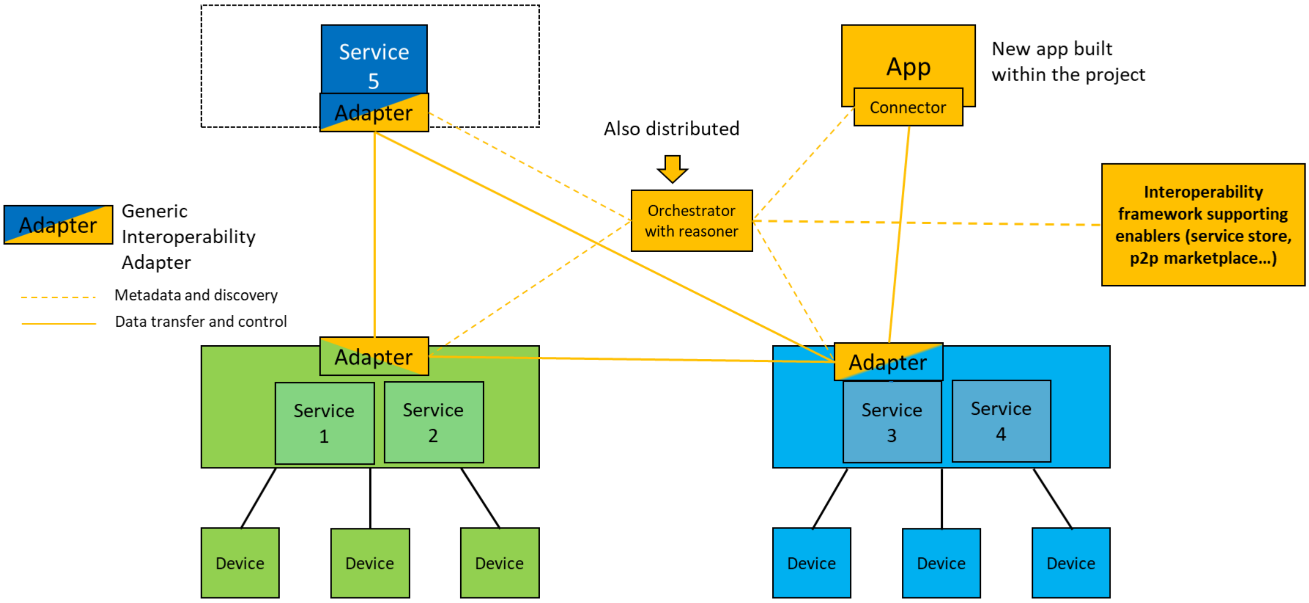
Service 5
Adapter
App
Connector
New app built within the project
Also distributed
Orchestrator with reasoner
Adapter
Generic Interoperability Adapter
Interoperability framework supporting enablers (service store, p2p marketplace…)
Metadata and discovery
Data transfer and control
Adapter
Service 1
Service 2
Adapter
Service 3
Service 4
Device
Device
Device
Device
Device
Device

FIGURE 15 - IC SEMANTIC INTEROPERABILITY LAYER DISTRIBUTED ON THE PARTICIPATING DIGITAL PLATFORMS AND SERVICES

Figure 16 shows options for deploying Generic Adapter 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 Generic 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 [13].

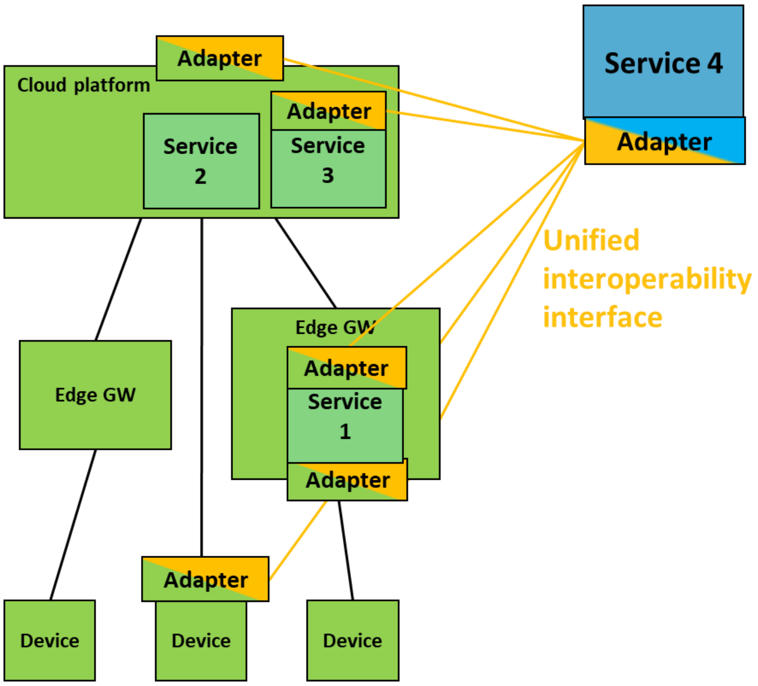

FIGURE 16 - DIFFERENT OPTIONS FOR DEPLOYING IC INTEROPERABILITY ADAPTER INSTANCES

4.2.3 ARCHITECTURE OF THE INTERCONNECT SEMANTIC INTEROPERABILITY LAYER

In this section we provide high level technical specification of the Interoperability Framework's SIL architecture focusing first on its three main building blocks, and then on presenting a complete interoperability path between two interoperable services. The main components of the SIL are:

- Knowledge Engine as the main enabler for semantic interoperability and reasoning capabilities within and between semantically interoperable ecosystems;
- Generic Adapter as the integration gateway between services and the Interoperability Framework including the Knowledge Engine;
- Service Specific Adapter as the configuration point for legacy services and their interfacing technologies.

KNOWLEDGE ENGINE

The Knowledge Engine (KE, see Figure 17) is a technology aimed at providing semantic interoperability by means of two features: *translation* and *discovery*. Both of 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 if 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.

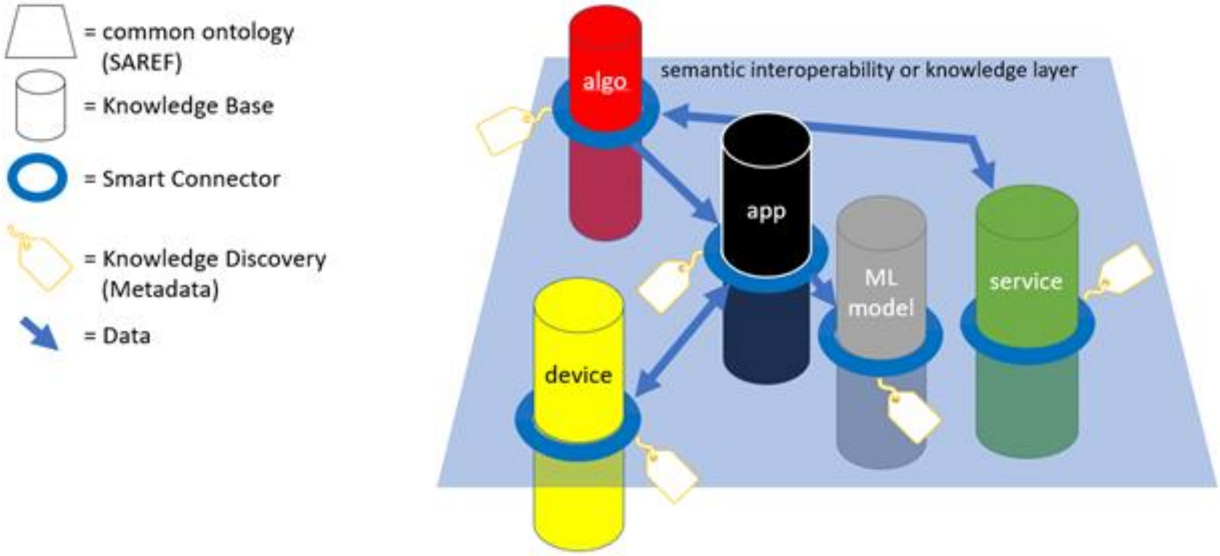
= common ontology (SAREF)
= Knowledge Base
= Smart Connector
= Knowledge Discovery (Metadata)
= Data
semantic interoperability or knowledge layer
algo
app
ML model
service
device

FIGURE 17 - KNOWLEDGE ENGINE CONCEPTUAL APPROACH

The Knowledge Engine should meet the following requirements: 1) fully utilize semantic web technology, 2) incorporate privacy and security by design, 3) support data pull and push.

A typical semantic web interoperability solution consists of a centralized triple store in which Extract, Transform, Load (ETL) processes are used to fill the triple store with data from different sources. Although this type of solution supports all typical semantic web benefits like flexible question answering and reasoning to infer new data, it is incompatible with requirements 2) and 3). The centralized triple store gives rise to privacy and security concerns and therefore both home and service owners are hesitant (if not resistant) in giving up their data. Apart from the privacy and security issues, this typical semantic web interoperability solution only supports data pull through querying and data push is typically not available.

The use cases within the InterConnect project rely heavily on data exchange and the interoperability layer should not hinder the willingness to do so due to privacy and security concerns. Apart from that, some of the InterConnect use cases also have more in common with control loops than information systems and so are more easily described using data push mechanisms than pull. With these considerations in mind, we have designed the Knowledge Engine that allows the semantic interoperability layer to benefit from the querying and reasoning capabilities of semantic web technologies, while supporting both data pull and push and being as distributed as possible.

Central to the design of the Knowledge Engine is the concept of a **Knowledge Base (KB)** (depicted as blue circles in Figure 17). A KB is a logical unit where knowledge flows to and/or from. These KBs can be anything like apps, services or existing databases and their nature depends on the use case that is being implemented. Also, the size of a KB is flexible, it can represent a single device or a whole platform with multiple devices and services.

As shown in Figure 18, each KB instantiates a **Smart Connector (SC)** which allows it to register its capabilities and exchange data with other KBs connected to the **Knowledge Network (KN)**. The SC is the generic software component that does all the heavy lifting within the Knowledge Engine. Each SC registers itself in a **Knowledge Directory (KD)** with a description of the capabilities that it wants to make available to other SCs. These KB capabilities supported by the SC are called **Knowledge Interactions (KI)**. Each KI is a capability description of the KB and each KB has one or more KIs. There are four types of KIs: **Ask, Answer, Post and React**. Both the Ask/Answer and Post/React are opposites of each other where the Post and Ask Knowledge Interactions represent the capability of the KB proactively posting or asking data to/from the KN. While the React and Answer KIs represent the capability of the KB reactively reacting to or answering a question from a Post or Ask, respectively.

A KI also contains one or two **graph patterns** (depending on its type) that uses the terminology from a common ontology to describe the actual type of data that the KB produces or consumes. The Ask and Answer KI expects a single graph pattern, while the Post and React require a single argument graph pattern, but optionally allow a result graph pattern as well. These graph patterns use a subset of the SPARQL syntax[10] and an example looks like this:

?mm rdf:type saref:Measurement .

?mm ex:hasValueInCelcius ?v .

This graph pattern could be used in combination with the Post KI for a sensor KB that regularly publishes measurements of the temperature in degrees Celsius. These types of KIs together with the graph patterns cover most data exchange scenarios necessary for realizing the InterConnect pilots. After a KB has register its capabilities using KIs, the data exchange starts depending on their types.

- In case of an **Ask KI**, the KB is expected to proactive trigger the Smart Connector to ask the registered question optionally providing bindings for the variables in its graph pattern. Any KB that can answer such questions will be involved by the SC.
- In case of an **Answer KI**, the KB will be contacted by its SC whenever another KB asks the type of data it can provide.
- In case of a **Post KI**, the KB can post data to its SC whenever it sees fit. Any KB with compatible KIs will get a chance to react to the publication of data.
- In case of a **React KI**, the KB will be contacted by its SC whenever another KB posts data to which it wants to react.

In short, a SC of KB A will involve any other KB B that has compatible capabilities with any of the capabilities of KB A. In the front of semantic reasoning the Knowledge Engine supports two approaches for checking KI compatibility and executing knowledge discovery and exchange:

- **Graph pattern matcher –** this is approach where KIs will execute knowledge exchange only if the graph patterns completely match. This approach ensures high speed knowledge exchanges.
- **Semantic reasoner –** this approach will ensure knowledge exchange through KIs with graph patterns that do not necessarily match completely. Partial matching is enabled and with it, new knowledge inference is possible in a wide Knowledge Network. The semantic reasoner is slower than the matcher, but it provides more flexibility in defining graph patterns for KBs.

The Knowledge Engine Runtime comprises a set of Smart Connectors and internal interfaces needed for facilitating KIs between KBs. This KE Runtime can be deployed on different system levels: on level of single service runtime, on a level of one digital platform, shared among multiple services and digital platforms (e.g. on a pilot level) and on a global/project level. This flexibility in deploying KE Runtime constitutes the distributed nature of the Interoperability Framework.

[10] https://www.w3.org/TR/rdf-sparql-query/#BasicGraphPatterns

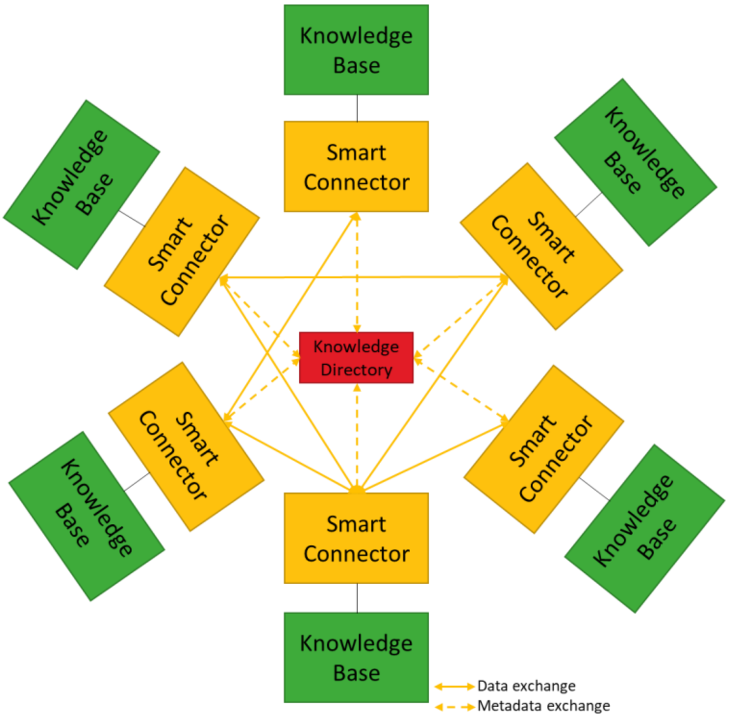

FIGURE 18 - KNOWLEDGE ENGINE HIGH LEVEL ARCHITECTURE

Before addressing the specification of the InterConnect adapters, we introduce the main terminology which might be a bit confusing to 3rd parties. From a perspective of a service, there are three main adapter concepts (see Figure 19):

- Service Specific Adapter (SSA) – configuration/mapping point between legacy interface and data model of the service and the InterConnect SIL.
- Generic Adapter (GA) – a generic software component that provides communication gateway for secure and trusted integration into a wider Interoperability Framework instance.
- InterConnect Service Adapter – a combination of SSA and GA representing a semantically interoperable service in a wider InterConnect Interoperability Framework instance (e.g. within and between project pilots).

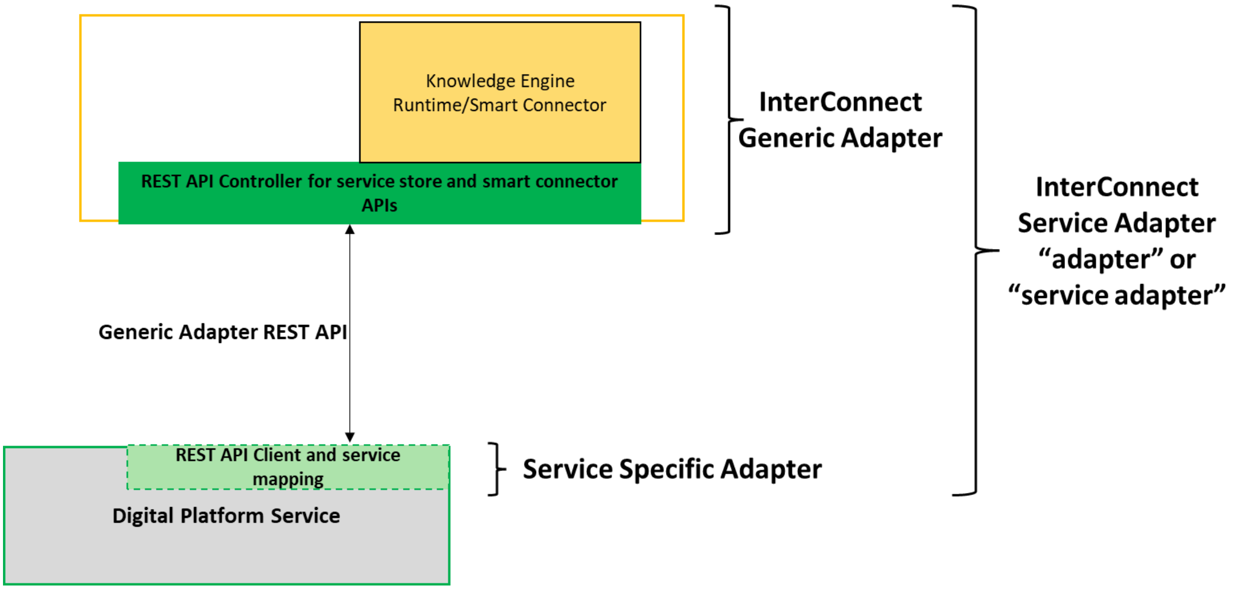
Knowledge Engine Runtime/Smart Connector
REST API Controller for service store and smart connector APIs
InterConnect Generic Adapter
InterConnect Service Adapter "adapter" or "service adapter"
Generic Adapter REST API
REST API Client and service mapping
Digital Platform Service
Service Specific Adapter

FIGURE 19 - TERMINOLOGY OF THE INTERCONNECT ADAPTERS

GENERIC ADAPTER

The Generic Adapter (GA) implemented within WP5 is defined based on requirements extracted from the digital platform catalogue (presented in Annex 1 – Digital Platform catalogue. The GA is a software gateway for secure and trusted communication between a service and a wider Interoperability Framework instance (see Figure 20). The GA provides unified REST API towards Service Specific Adapter. This GA REST API ensures communication with the Service Store (more details in section 4.3) for authentication and authorization of the service and the GA itself with the central identity provider. The GA also presents a valid interoperability compliance certificate when registering corresponding service and its knowledge capabilities in the Knowledge Engine. This constitutes the trust process behind the GA and service it represents. The GA REST API also facilitates interactions with the SIL (Knowledge Engine instance) by providing methods for KB and KI registration and also methods for executing KIs and corresponding knowledge exchanges. Each KI must be authorized before being supplied to the corresponding Smart Connector. The GA can integrate KE Runtime (or a single smart connector) and provide to integrators a single software artefact for instantiating InterConnect Semantic Interoperability Layer. To recap, the GA enables:

- A unified and secured communication interface using REST API;
- Authentication and authorization point for IF access;
- Deployment flexibility – Docker, with and without Knowledge Engine Runtime;
- Automates registration of knowledge base and common knowledge interactions on boot.

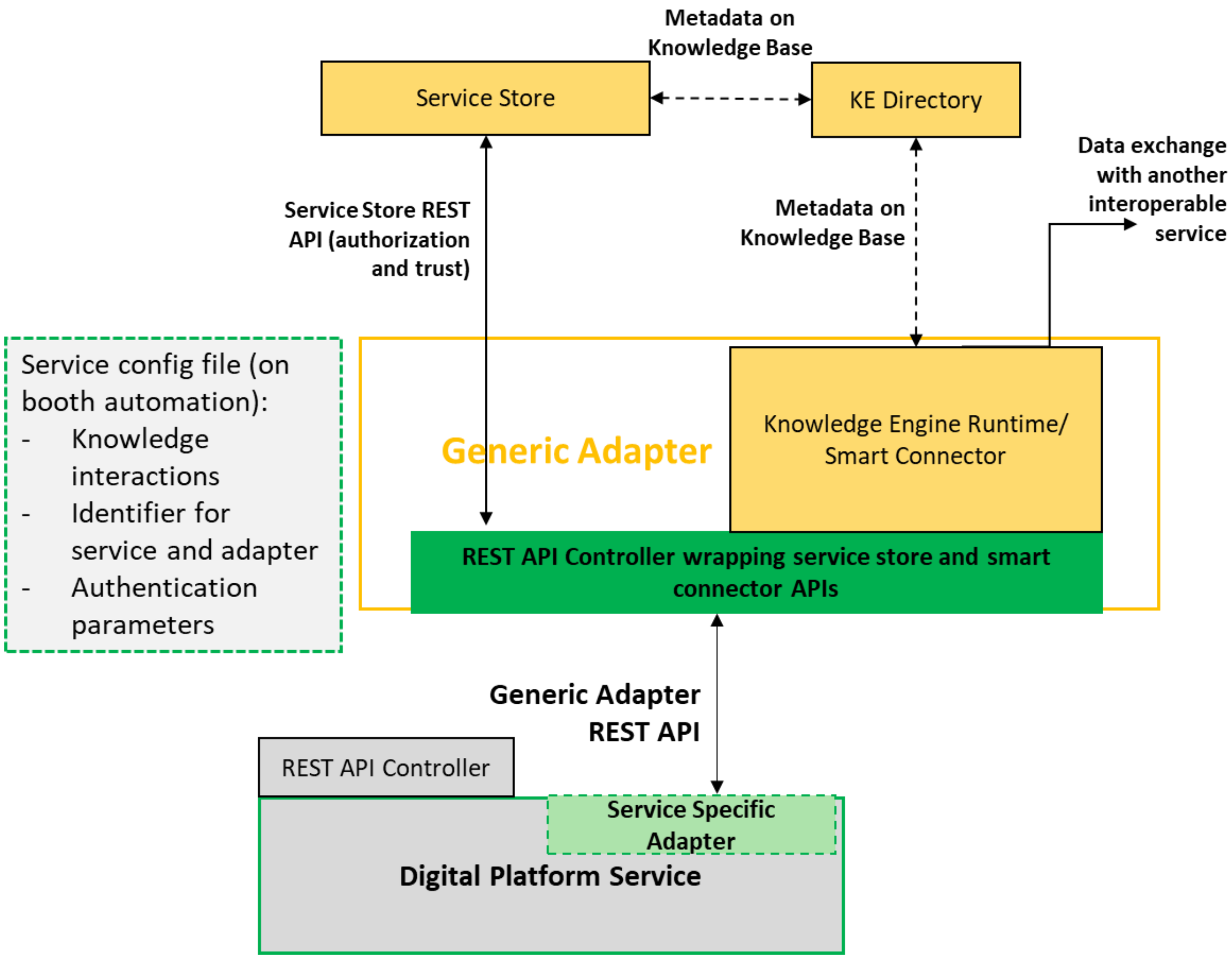
Metadata on Knowledge Base
Service Store
KE Directory
Data exchange with another interoperable service
Service Store REST API (authorization and trust)
Metadata on Knowledge Base
Service config file (on booth automation):
- Knowledge interactions
- Identifier for service and adapter
- Authentication parameters
Generic Adapter
Knowledge Engine Runtime/ Smart Connector
REST API Controller wrapping service store and smart connector APIs
Generic Adapter REST API
REST API Controller
Service Specific Adapter
Digital Platform Service

FIGURE 20 - HIGH LEVEL ARCHITECTURE OF THE GENERIC ADAPTER

SERVICE SPECIFIC ADAPTER

The Service Specific Adapter (SSA) is a custom software component developed and configured for a specific service/Knowledge Base. Each service provider goes through a process of implementing SSA. The main functionalities of the SSA are:

- SSA Service endpoint functionality – includes all necessary functionality to interact with the service via the offered (legacy) service API.
- SSA mapping functionality – performs mapping of parameter bindings (semantic interface) to service API parameters and vice versa. Can be one-to-one mapping or more complex logic to combine for instance several API calls to complete one binding set.
- SSA GA endpoint functionality:
    - Register the Generic Adapter instance for this service.
    - Register the Knowledge Base - this creates a smart connector.
    - Register the Knowledge Interactions (Graph Patterns).
    - Offer Knowledge Interaction execution.

A methodology is provided on how to customize (or generate new) SSA and its interaction with the Generic Adapter for interfacing technologies not available in the Interoperability Framework. This way the library of available service specific adapters will continue to grow during and after the project. This extensive library will be available for future integrators to choose from based on the services closest to their service specifications. This will drastically streamline the process of onboarding new services and systems into the semantically interoperable ecosystems established by the project.

Figure 21 shows the conceptual architecture of a Knowledge Base. Three key functionalities can be distinguished. At the right, there is the GA that establishes the connection with the Interoperability Framework (i.e. the Smart Connector of the Knowledge Engine). At the left, there is the to-be-made-interoperable component, which can be a physical device/appliance, or a software functionality/service (e.g. forecaster, optimiser). In the middle, there is the SSA that contains the actual logic that implements he ontology-based semantic interaction scheme and data models: it implements parameter binding and mapping of Graph Pattern parameters to to-be-made-interoperable component parameters.

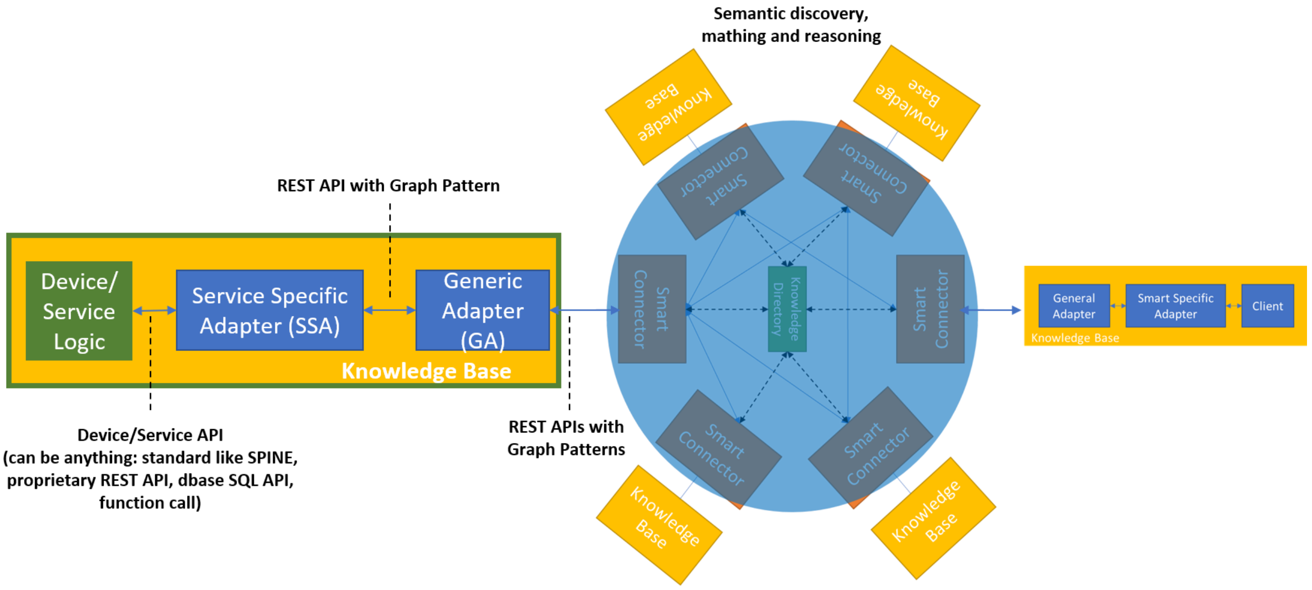

FIGURE 21 - KNOWLEDGE BASE WITH ITS SSA AND GA

INTEROPERABILITY CHAIN

All together, these SIL components facilitate a knowledge exchange between two interoperable services (Knowledge Bases). In Figure 22 there are two services with corresponding SSAs, GA and smart connector of the Knowledge Engine. This makes them semantically interoperable. The figure also depicts the Service Store as the main identity and trust provider and Knowledge Directory as facilitator of semantic discovery.

The first message exchange segment depicts the process of service registration and onboarding into the Service Store and Knowledge Engine. This creates secure setup for further knowledge exchanges. The next segment relates to registration of capabilities of each service for data provision and consumption (Knowledge Interactions – KI). The Knowledge Directory keeps record of all KBs and KIs so that Smart Connectors can consult it in order to discover appropriate end points for data exchange.

The data/knowledge exchange segment depicts the process of mapping service data requests or instructions onto corresponding KIs. Based on KI and supplied graph pattern(s), the Smart Connector performs reasoning in order to select the Smart Connector of the appropriate service/Knowledge Base with which to execute knowledge exchange. The data payloads are going only between Smart Connectors. This means, that choosing where to deploy Smart Connectors (and Knowledge Engine Runtimes) needs to be guided by the privacy protection principles. Actual data payloads are never sent to centrally hosted components of the Interoperability Framework (Service Store and Knowledge Directory).

The figure also depicts a simple message flow between the Service Store and the Knowledge Directory for the functionality of Knowledge Explorer which allows users to overview all instances of knowledge Engine and registered KBs and their KIs.

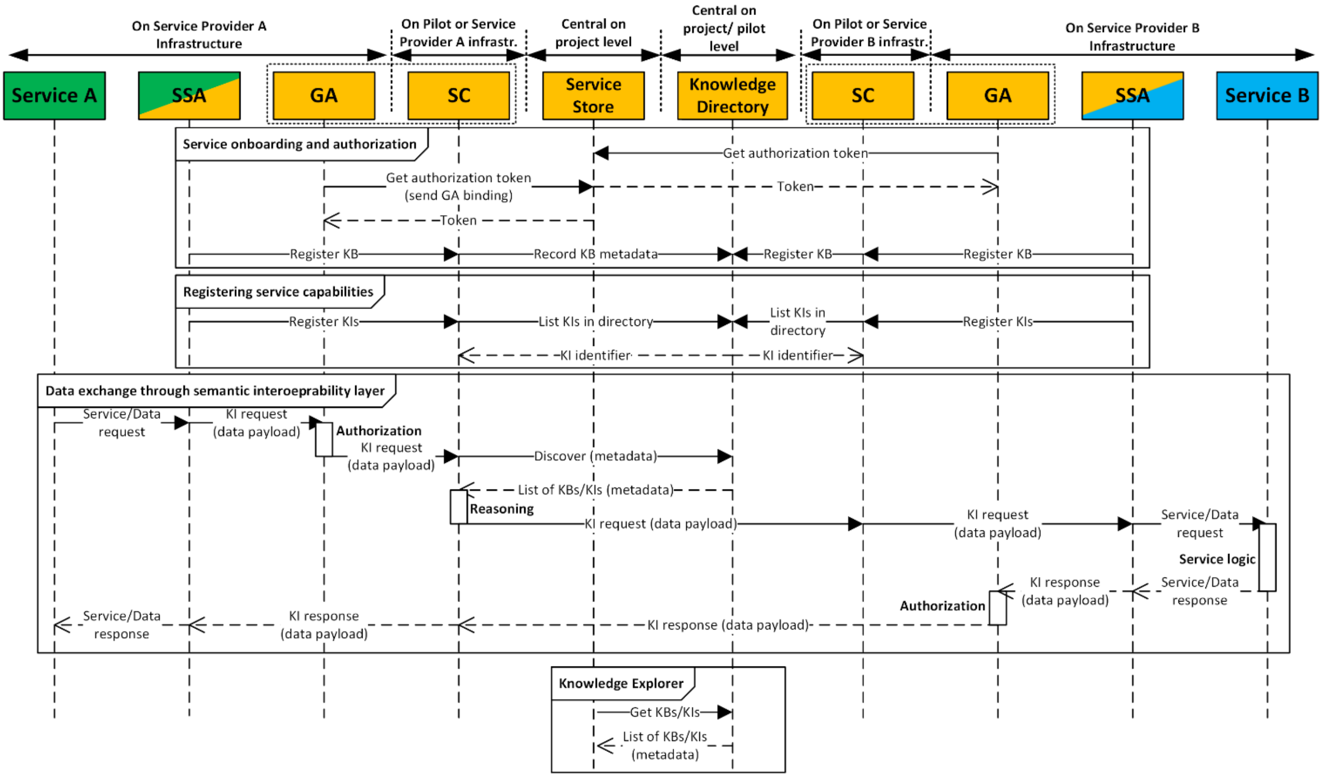
On Service Provider A Infrastructure
On Pilot or Service Provider A infrastr.
Central on project level
Central on project/ pilot level
On Pilot or Service Provider B infrastr.
On Service Provider B Infrastructure
Service A
SSA
GA
SC
Service Store
Knowledge Directory
SC
GA
SSA
Service B
Service onboarding and authorization
Get authorization token
Get authorization token (send GA binding)
Token
Token
Register KB
Record KB metadata
Register KB
Register KB
Registering service capabilities
Register KIs
List KIs in directory
List KIs in directory
Register KIs
KI identifier
KI identifier
Data exchange through semantic interoeprability layer
Service/Data request
KI request (data payload)
Authorization
KI request (data payload)
Discover (metadata)
List of KBs/KIs (metadata)
Reasoning
KI request (data payload)
KI request (data payload)
Service/Data request
Service logic
KI response (data payload)
Service/Data response
Authorization
KI response (data payload)
KI response (data payload)
Service/Data response
Knowledge Explorer
Get KBs/KIs
List of KBs/KIs (metadata)

FIGURE 22 - INTEROPERABILITY CHAIN AND MESSAGE SEQUENCE CHART BETWEEN TWO INTEROEPRABLE SERVICES

The data exchange segment of the flow diagram can be executed on the wider scale, not just between two services. This discovery, reasoning and Knowledge Interactions for knowledge exchange will happen on the level of whole project pilots and also between the pilots and on global/project level, depending on configuration of the interoperability Framework instances.

4.3 INTERCONNECT SERVICE STORE

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 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 (KE 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 is defined between WP2-WP3-WP5 as the SAREFization process.

All project partners who are service providers will onboard their services onto the service store and create the first catalogue of interoperable services. 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 23.

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.

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 (e.g., authorization for whose services may have enabled interaction). Access control might also include other types of subscriptions for service usage. The complete set of access control parameters will be specified based on information obtained from WP3 and it will be documented in the official deliverable D5.4 (end of 2021) as well as in the Service Store release material.

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.

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. 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.

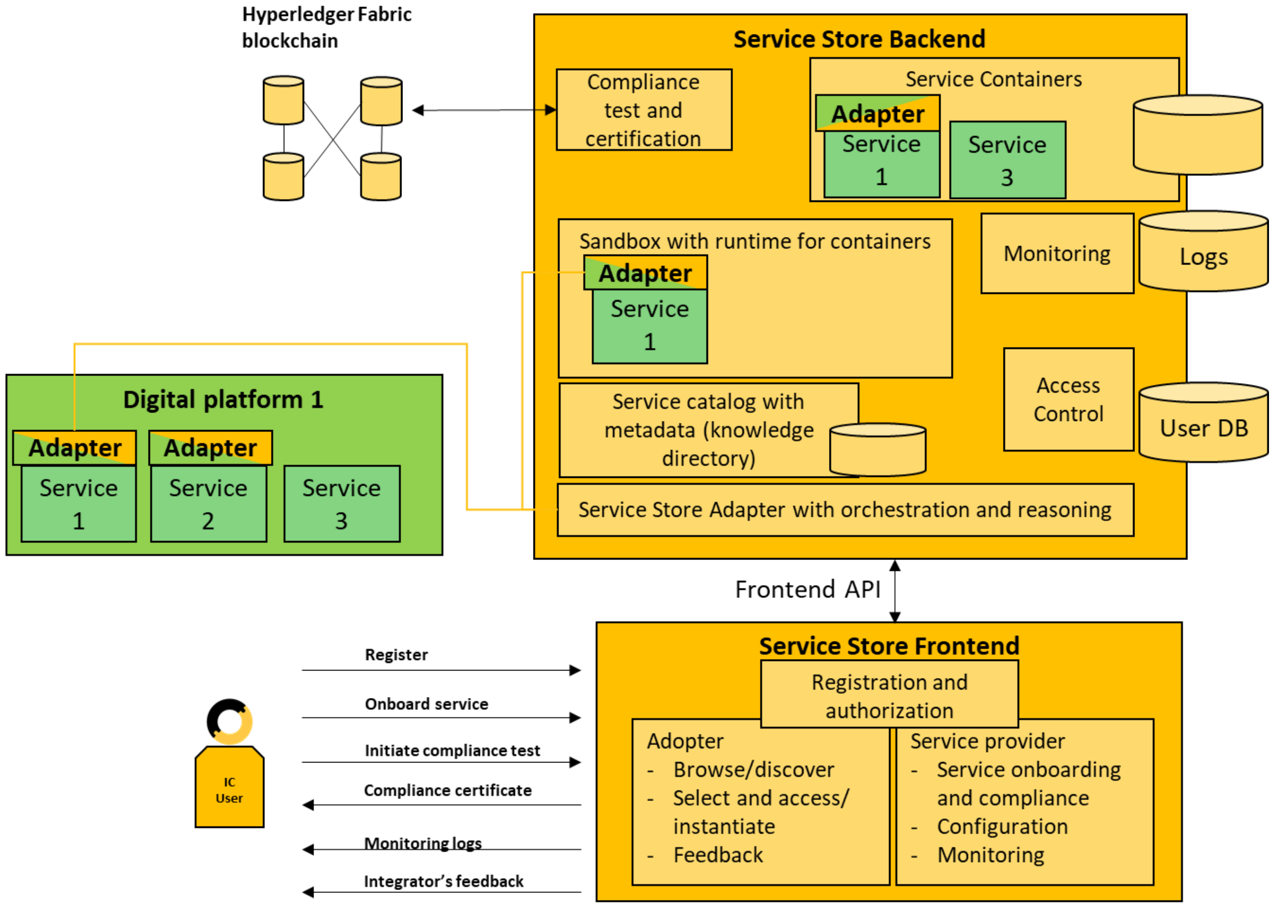

FIGURE 23 - IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES PROVIDED FOR SERVICE PROVIDERS

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 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 track 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.

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 24.

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 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, notably 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.

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.

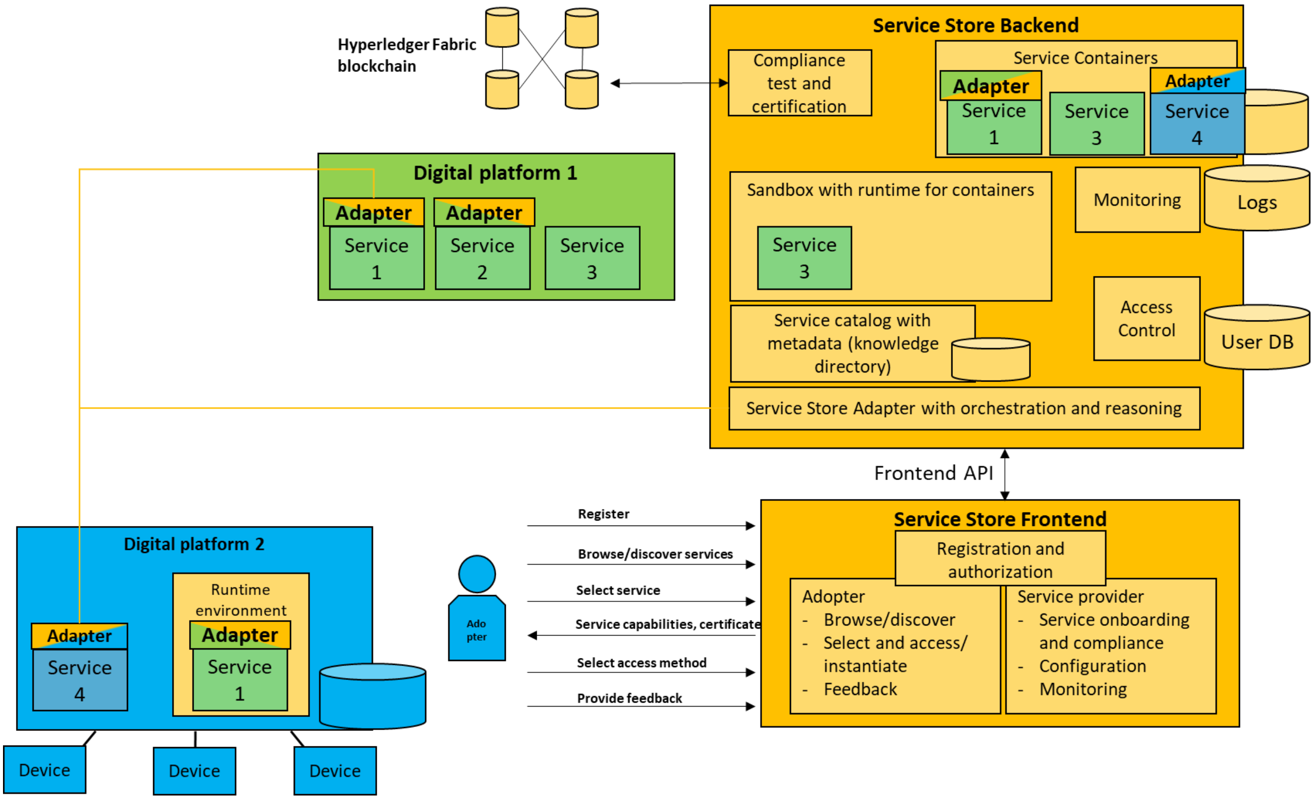

FIGURE 24 - IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES PROVIDED FOR SERVICE ADOPTERS

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:

- The **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.
- The **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.

Services offered through the IC service store can be accessed in three ways[11]:

- **Service hosted on originating digital platform**:
    - Access through corresponding interoperability adapter.
    - 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.

[11] The actual choice of supported service provision options will be an implementation decision made by service provider.

- **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, unlocking access to the semantic interoperability layer.
    - Service adopter manages all access control and data/privacy protection procedures.

The IC service store will provide a web-based frontend with a graphical user interface in support of the provided functionalities to all users. The service store frontend will utilize the corresponding REST API provided by the web framework implemented in the service store backend. Figure 25 shows high level UML usage flow diagram for the IC service store web frontend.

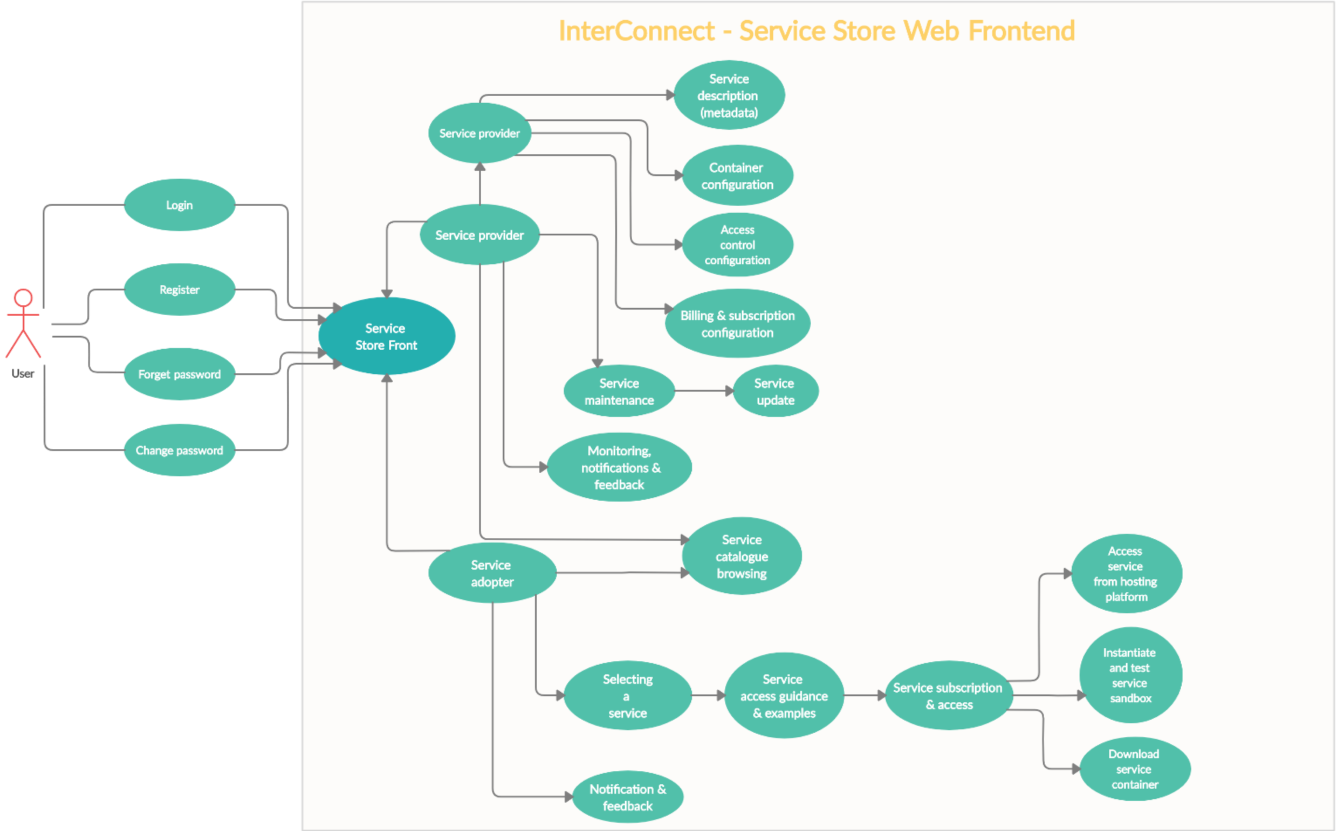
InterConnect - Service Store Web Frontend
User
Login
Register
Forget password
Change password
Service Store Front
Service provider
Service provider
Service description (metadata)
Container configuration
Access control configuration
Billing & subscription configuration
Service maintenance
Service update
Monitoring, notifications & feedback
Service catalogue browsing
Service adopter
Selecting a service
Service access guidance & examples
Service subscription & access
Access service from hosting platform
Instantiate and test service sandbox
Download service container
Notification & feedback

FIGURE 25 - UML USAGE FLOW DIAGRAM FOR THE IC SERVICE STORE WEB FRONTEND

The IC service store will be developed using Java (backend) and Angular (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 prove necessary for addressing the regulatory constraints and other business-related requirements.

Final functionality of the Service Store will be automated interoperability compliance check for services during the onboarding process. The interoperability compliance test should check syntactic and semantic interoperability or the ability of an interoperable service to exchange data through interoperability layer (utilizing generic adapters) and ability to understand and properly act on received data and knowledge represented within. For this purpose, the WP3 should clearly categorize all services into predefined categories. Each category should correspond to the part of the SAREF based project ontology. This should precisely define semantic compliance checks focusing on relevant parts of the adopter ontology. Figure 26 depicts high level flow of the interoperability compliance test. The project will employ **interoperability compliance certificates** to be facilitated by private permissioned blockchain and smart contracts. The compliance certificates will ensure that the InterConnect interoperable ecosystems can choose services and other digital system with trusted level of interoperability compliance to join. The certification on blockchain architecture is the basis for building InterConnect trustworthiness processes for future ecosystem scaling outside the consortium.

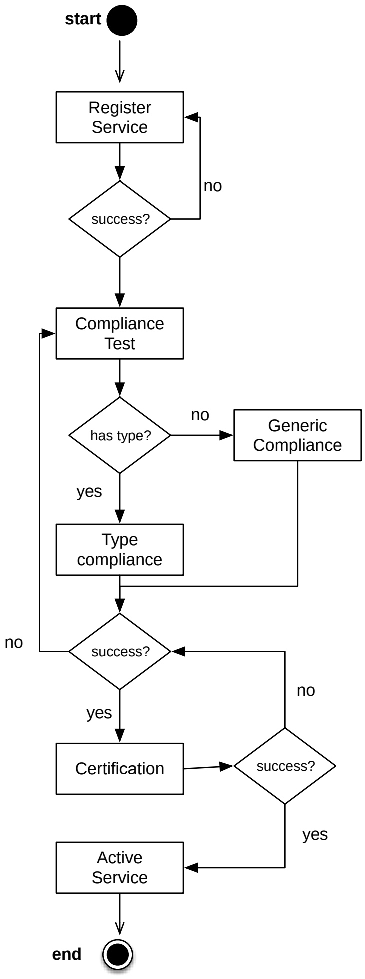

FIGURE 26 - PRELIMINARY HIGH-LEVEL FLOW OF INTEROEPRABILITY COMPLIANCE TEST

4.4 P2P MARKETPLACE ENABLERS

A peer-to-peer or P2P marketplace is created as platform 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[12], Uber[13], Etsy[14], OpenBazaar[15], etc.

Proliferation of distributed energy resources (photovoltaic panels, electric vehicles, smart appliances, and battery storage systems) paved the way for P2P energy marketplaces. The 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.

Within InterConnect, we will pursue **distributed ledger technologies**, and more specifically, consortium and private permissioned **blockchain-based on Hyperledger Fabric**. Hyperledger Fabric is an enterprise-grade, distributed ledger platform that offers modularity and versatility for a broad set of industry use cases. The modular architecture for Hyperledger Fabric accommodates the diversity of enterprise use cases through plug and play components, such as consensus, privacy, and membership services. This technology allows establishing P2P marketplaces where certain levels of regulation and organization are 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 energy trading, flexibility and power profile aggregation, carbon emission trading, loyalty tokens, energy provenance tracking, amongst others.

Figure 27 provides the high-level architecture of InterConnect's P2P marketplace. **The P2P marketplace can be an energy marketplace or a marketplace for data transactions required for the 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 4.2. This can be achieved with supporting data ingestion services which are equipped with Generic 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. The 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. Order matching engine is responsible for matching offers and orders following the transaction logic defined by the marketplace facilitators and applying relevant regulations.

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

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

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

[15] https://openbazaar.org/

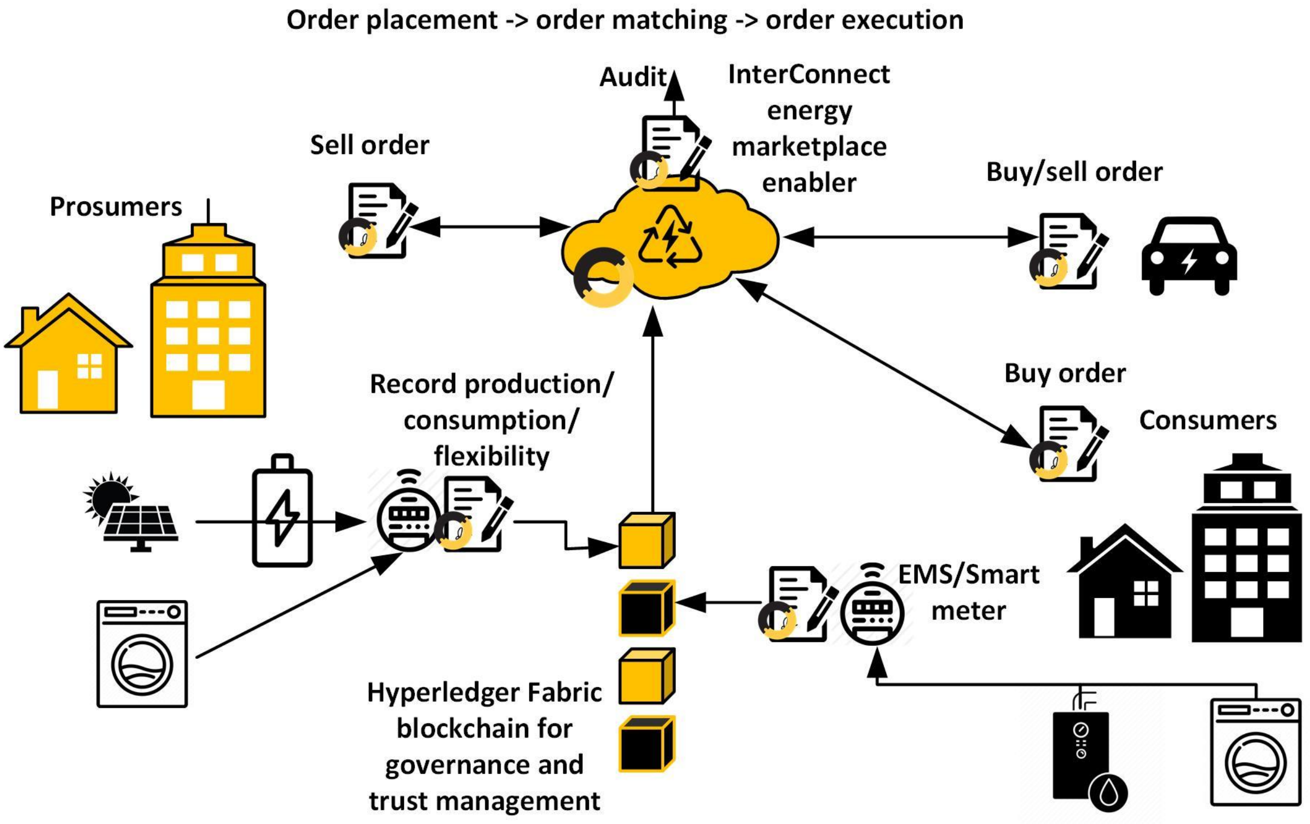
Order placement -> order matching -> order execution
Audit
InterConnect energy marketplace enabler
Sell order
Buy/sell order
Prosumers
Buy order
Consumers
Record production/ consumption/ flexibility
EMS/Smart meter
Hyperledger Fabric blockchain for governance and trust management

FIGURE 27 - INTERCONNECT P2P MARKETPLACE ENABLERS AND INSTANTIATION EXAMPLE

In the InterConnect project we tackle the P2P marketplace development in T5.4. 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 in the project pilots. The P2P marketplace enablers include (see Figure 28):

- **Hyperledger Fabric blockchain configurations** for different types of P2P marketplaces (different hierarchies, consortium organizations, stakeholders, nodes and channels).
- **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.
    - Smart contract implemented as semantic interoperability adapter for interfacing with the wider InterConnect Interoperability Framework.
    - Smart contracts for registering and identifying key actors and resources constituting P2P marketplaces.
    - Smart Contracts for integration of interoperable services which write data to or read data from the Hyperledger Fabric. This ensures that the P2P marketplaces are integrated with a wider instance of Interoperability Framework.
- **Configurable order matching 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.

- **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.

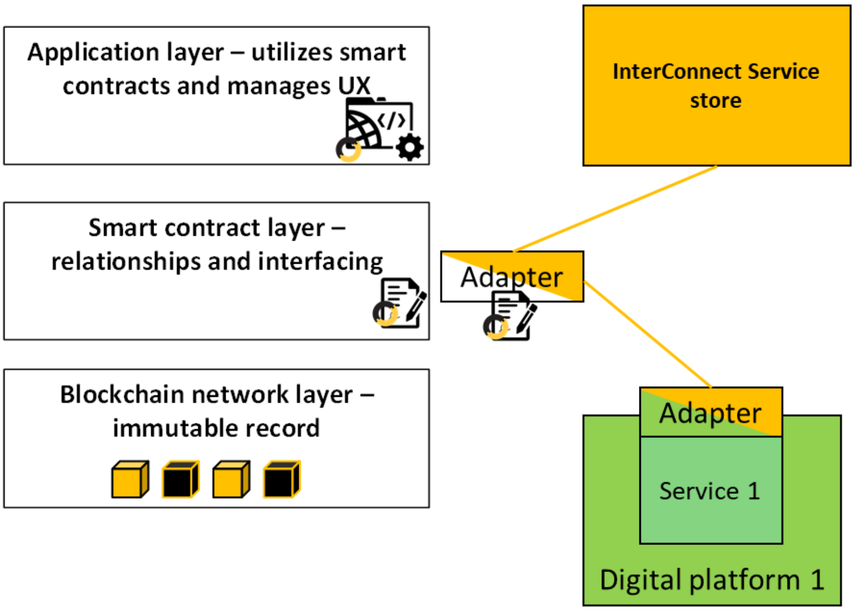
Application layer – utilizes smart contracts and manages UX
Smart contract layer – relationships and interfacing
Blockchain network layer – immutable record
InterConnect Service store
Adapter
Adapter
Service 1
Digital platform 1

FIGURE 28 - INTERCONNECT P2P MARKETPLACE ENABLERS

The Interoperability Framework provides these P2P marketplace enablers as part of its toolbox. The enablers are provided as deployable containers that allow pilot owners and integrators to deploy and fully manage P2P marketplace instances. The established P2P marketplaces are in **full control and under jurisdiction** (regulatory, market wise, data privacy protection) **of the integrators**. One or multiple blockchains can be established on the level of the 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. As the number of P2P marketplaces deployed in the pilots increases, the set of validated P2P marketplace enabler configurations will be enhanced and made available to 3rd party integrators to consider when making plans for their own P2P marketplace instances.

In the given SoTA of P2P energy marketplaces, multiple stakeholders can be named: end-users, Home Energy Management Systems (HEMS), Flexibility Aggregators (FAs), Retailers, (Renewable) Energy Communities ((R)ECs), (R)EC Managers, Balance Responsible Parties (BRPs), DSOs, TSOs, Service Providers (e.g., Forecasters) and Market Operator. Among these some might have an active trading role (HEMS, RECs, Retailers), some might have management roles (REC Managers, Market Operator), some might provide “ground truth” required to verify data and transactions (DSOs, TSOs), some will provide balancing services to the grid (BRPs, FAs), while some might just need access to energy usage data to provide other services (Forecaster). Some P2P marketplaces might have the use for all these roles, while others will only need a subset. To fulfil their many goals, stakeholders would have to actively collaborate with others.

Because of this, a generalized design with pluggable components (organizations, channels, services) is required. HF is an excellent candidate to support a plethora of use-cases that can be derived from the description above. It offers **privacy-by-design, secure and controlled access control on multiple levels and physical and logical separation of access to data**.

Figure 29 shows an example 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 order matching engine which is responsible for managing execution of transactions in with predetermined rules.

For the InterConnect project, fast prototyping, deployment, and validation of the private permissioned and consortium blockchains based on Hyperledger Fabric will be realized with ChainRider[16] blockchain as a service solution provided by the WP5 leader and T5.4 leader, VizLore Labs Foundation.

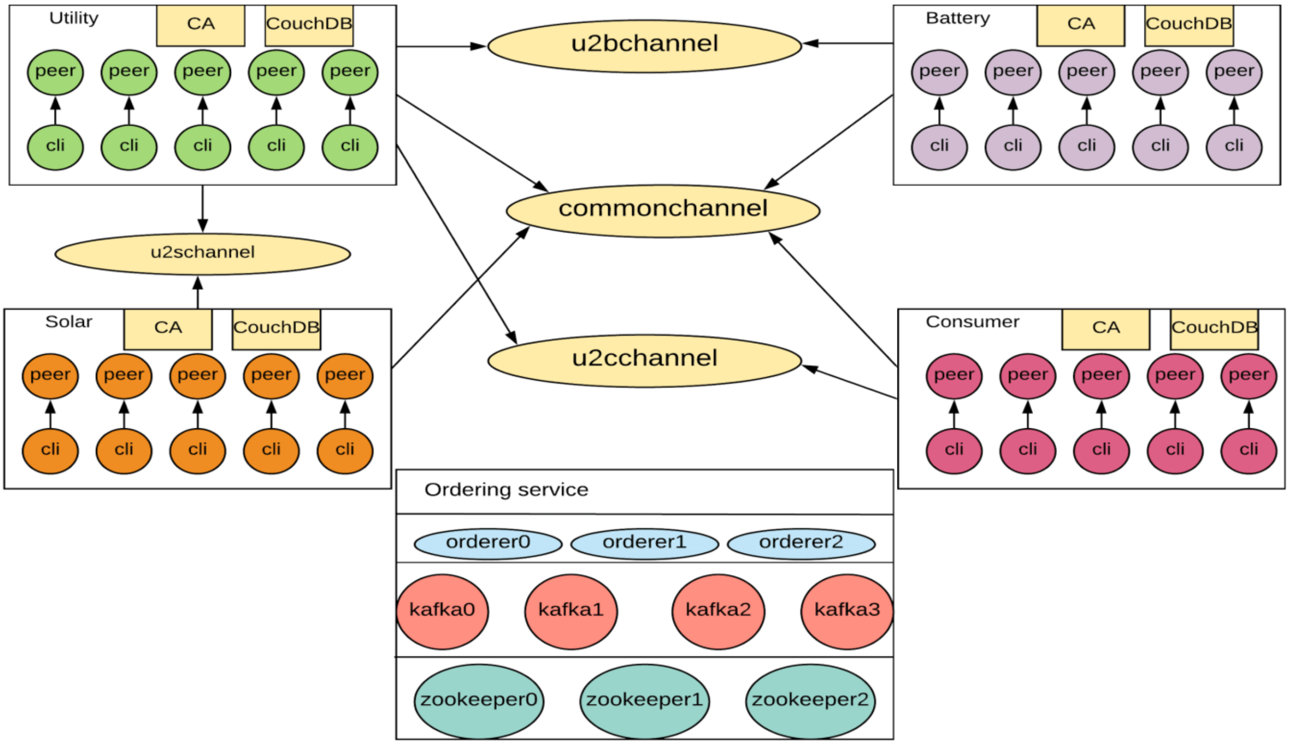

FIGURE 29 - EXAMPLE ORGANIZATION OF HYPERLEDGER FABRIC ARCHITECTURE FOR TRUSTED DATA TRANSACTIONS

Figure 30 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 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.**

Lastly, 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 towards implementation of the DSO interface.

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

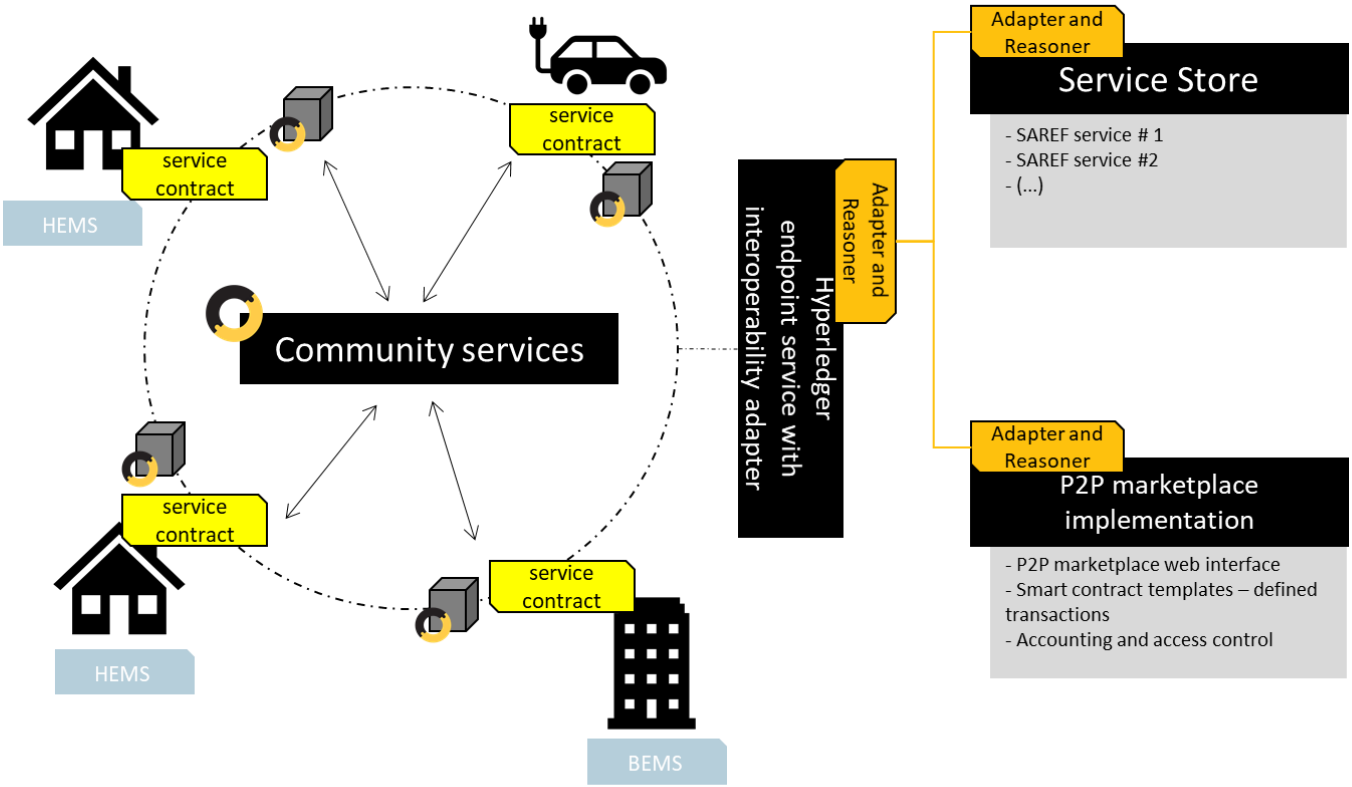

FIGURE 30 - INTEROPERABILITY OF THE INTERCONNECT SEMANTIC INTEROPERABILITY LAYER AND COMMUNITY BASED BLOCKCHAIN NETWORKS

4.5 SECURITY AND DATA PROTECTION FRAMEWORK

The InterConnect interoperability layer does not participate directly in operational data forwarding between services/endpoints equipped with generic interoperability adapters. This means that **the Interoperability Framework will not 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. Different deployment options of the Interoperability Framework (more specifically semantic interoperability layer and P2P marketplaces) draw different privacy protection jurisdiction boundaries. Integrators must be aware of these boundaries when choosing deployment option and then deciding to exchange potentially privacy sensitive data through the instantiated interoperability layer.

Specific security and privacy protection approach behind each digital platform are included into the WP5 catalogue[17]. 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 generic interoperability adapters and semantic reasoning procedures. Semantic discovery, reasoning, and data translation between legacy and SAREF based data models will include specified access control and privacy protection rules.

[17] See Annex 1 – Digital Platform catalogue.

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 (e.g., project pilots):

- InterConnect users register on the InterConnect Service Store and are recognized as authorized users for accessing IC's Interoperability Framework services. InterConnect user will feature:
    - A user ID for authentication, authorization for attribute-based access control.
    - All collected information will be encoded and stored in the InterConnect user database.
- An InterConnect endpoint (services, devices) is recognized as an authorized endpoint to participate in the InterConnect semantic interoperability layer and access the framework services (via the Generic Adapter).
    - Interoperable endpoints will have authorization ID for attribute-based access control.

Figure 31 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**. 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.

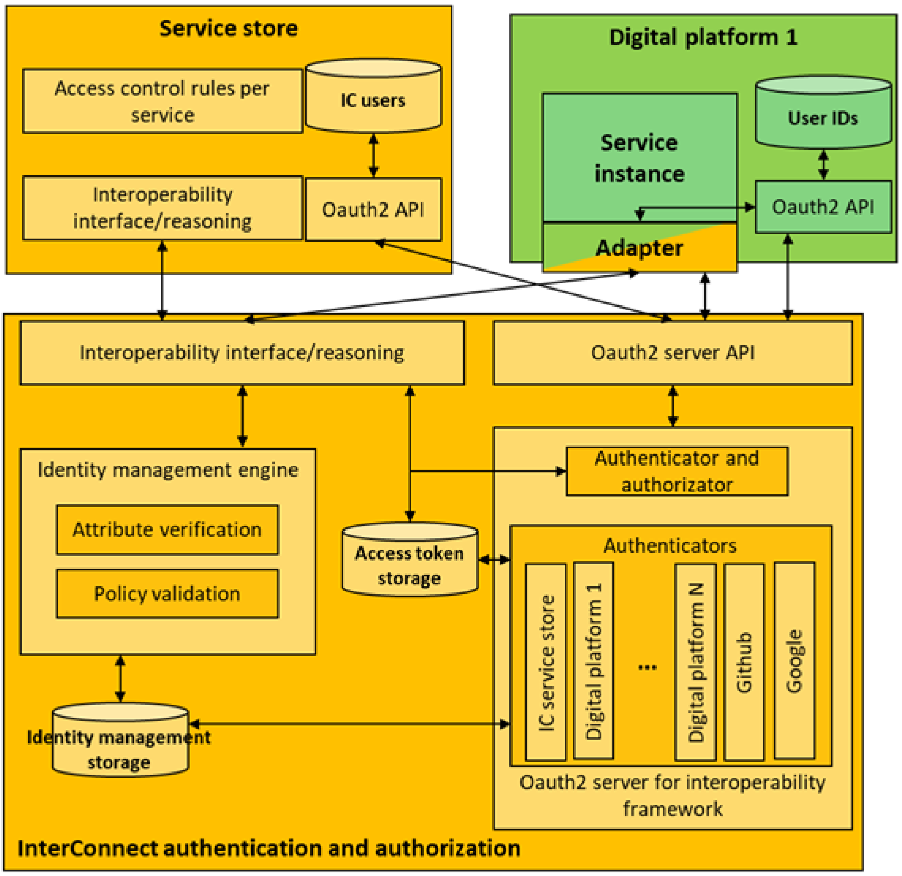
Service store
Access control rules per service
IC users
Interoperability interface/reasoning
Oauth2 API
Digital platform 1
Service instance
User IDs
Oauth2 API
Adapter
Interoperability interface/reasoning
Oauth2 server API
Identity management engine
Attribute verification
Policy validation
Access token storage
Authenticator and authorizator
Authenticators
IC service store
Digital platform 1
...
Digital platform N
Github
Google
Identity management storage
Oauth2 server for interoperability framework
InterConnect authentication and authorization

FIGURE 31 - ARCHITECTURE OF THE INTERCONNECT AUTHORIZATION AND ACCESS CONTROL ENABLER - EARLY DRAFT

The access control policies and identity attributes will be stored on the hosting digital platforms' Generic Adapter. 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 32. Options for authorizing users with 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.

Access control mechanisms can be specified on the level of the pilot or the whole project. Figure 32 shows a typical pilot architecture with two digital platforms each with its own set of access control rules and data protection frameworks. The semantic interoperability layer interconnects the two platform and their services. Users registered on the digital platform 1 can access only the services of the host digital platform. The same stands for a user of digital platform 2. An InterConnect user is authorized to access all interoperable services (if not specifically constrained by interoperable service provider). The InterConnect access control mechanism will enable end users of interoperable platforms to be authorized as InterConnect users. With the user profile from the home digital platform, user can access Interoperability Framework services and other interoperable services available in the service store. The authentication and authorization are facilitated by generic interoperability adapter as the gateway into semantically interoperable ecosystems.

The InterConnect access control will allow service providers to enforce access control rules in line with their data protection policies and business models. The privacy protection mechanism will also be employed as part of the semantic interoperability layer and its adapters/connectors. Consortium will investigate options to introduce privacy sensitivity categories for data model attributes and parts of the ontology indicating the level of privacy protection which needs to be followed while transferring, storing, and processing data exchanged in the applied data model.

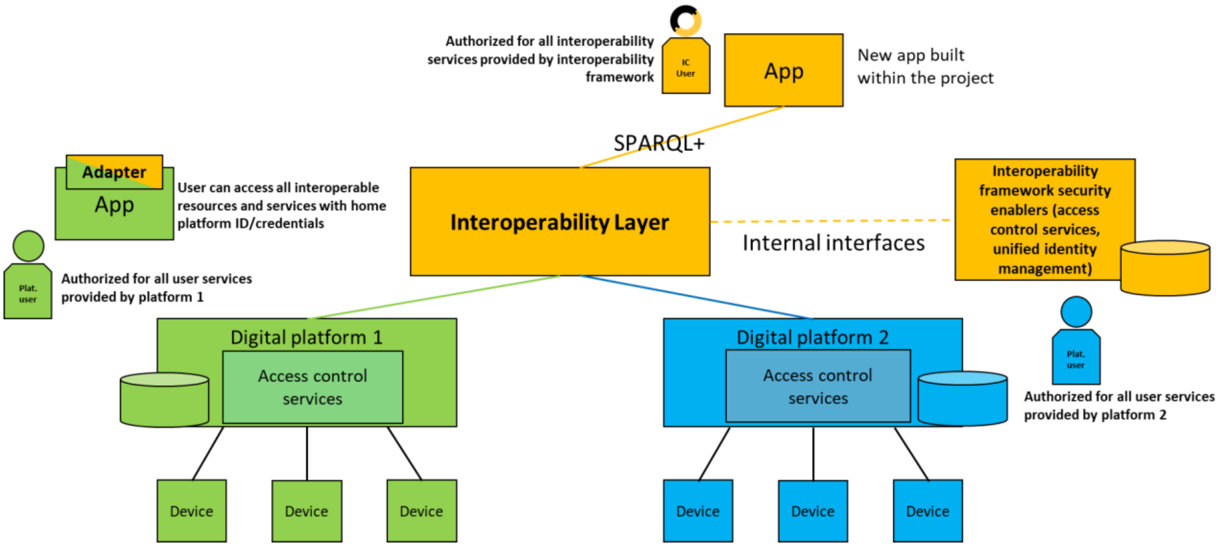
Authorized for all interoperability services provided by interoperability framework
IC User
App
New app built within the project
SPARQL+
Adapter
App
User can access all interoperable resources and services with home platform ID/credentials
Interoperability Layer
Internal interfaces
Interoperability framework security enablers (access control services, unified identity management)
Plat. user
Authorized for all user services provided by platform 1
Digital platform 1
Access control services
Digital platform 2
Access control services
Plat. user
Authorized for all user services provided by platform 2
Device
Device
Device
Device
Device
Device

FIGURE 32 - INTERCONNECT ACCESS CONTROL MECHANISM INTEGRATED WITH SEMANTIC INTEROPERABILITY LAYER

This mechanism could 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. Regarding the security and privacy protection capabilities of the P2P marketplaces to be deployed in the pilots, the underlying technology Hyperledger Fabric provides a set of measures that can be configures and deployed per use case needs (integrator’s decision). The security protection measures of HF include:

1. **Transport Layer Security (TLS)** for all interfaces.

2. **Unique Identity** – membership service provider (MSP) guarantees the legitimacy of the organization and all or its users and applications on the blockchain. Organizations can use the HF native MSP, Certificate Authority Service, or connect their own MSP/identity provider.
3. **Policies** can be used on different levels. There are Channel Modification Policies (CMP), Chaincode Lifecycle Policies (CLP), and Chaincode Endorsement Policies (CEP). All of these govern rules about how different aspect of the blockchain must be managed. CMPs define rules such as: every change to a channel's configuration (e.g., adding a new member organization) must be agreed upon by all channel members. CLPs define rules such as: every chaincode on channel X must be endorsed (seen, checked & agreed on) by 2/3 channel members. CEPs define how many organizations, and their nodes must verify every transaction of the given chaincode.
4. **Controlled Blockchain Access** – Users and apps access blockchain resources within their own organizations by interacting with the SDK layer on top of the blockchain network. The SDK layer authenticates the user/app via its digital certificate.

The privacy protection measures of Hyperledger Fabric include:

1. **Multi-channel design** separates the information between different channels. Only organizations belonging to a certain channel can read and write information.
2. **Private data collections (PDC)** further refine privacy within a channel. In case of more organizations on one channel a PDC allows for a subset of them to share data privately. For use cases where private data only needs to be on the ledger until it can be replicated into an off-chain database, it is possible to "purge" the data after a certain set number of blocks, leaving behind only hash of the data that serves as immutable evidence of the transaction. This ability to delete or update data stored in blockchain is what ensures that deployed P2P marketplaces can be GDPR compliant (not possible with public blockchain approaches because of the strict immutability).
3. **Controlled Chaincode access** – users/apps can only access the chaincode on the channels their organization is part of.
4. **Controlled Data Access** – Within a chaincode, access to different functions (e.g., read, write, update) and parts of digital assets can be limited to allow only users/apps from certain organization or with certain attributes to invoke them. For example, only users with "admin" roles with the identity attribute "location=PT" can write new data, while users with "viewer" will be able to read data.

The complete process is specified and implemented within dedicated task (T5.3) of the WP5 and reported in D5.3 [14]. Data boundaries and message sequence diagrams for authorization are provided in D5.2 [13].

4.6 THE ROLE OF BLOCKCHAIN TECHNOLOGIES IN THE INTEROPERABILITY FRAMEWORK

Deploying the blockchain technology for facilitating trust and identity management in distributed systems is becoming a common practice. The InterConnect project takes advantage of the blockchain technology in three principal ways:

- **Interoperability compliance certification** with certificates written in private permissioned blockchain established on the project level. The Interoperability certification process will be performed when an interoperable service is onboarded into the InterConnect Service Store and also with each update on the service side, Interoperability certificate is referenced when building semantically interoperable ecosystems and whenever extending them with new services and stakeholders. The certificates provide means to validate interoperability compliance and interoperability capabilities of all participants in an Instance of the Interoperability Framework. This introduces interoperability into trustworthiness and data governance processes behind semantically interoperable ecosystems. More details on the process are presented in the section 4.3 on Service Store specification.

- **P2P marketplace enablers –** as described in section 4.5.
- **Knowledge exchange traceability** – this is the process of deploying private permissioned blockchain layer within semantically interoperable ecosystems so that each knowledge exchange can be linked with an agreement made between participating stakeholders. Each stakeholder participating in semantically interoperable ecosystem (defined by the instance of the Interoperability Framework) can establish knowledge exchange contracts with all other stakeholders with specific rules of engagement (to be negotiated and accepted by both/all parties). A smart contract facilitating different rules of engagement will be supplied. Before initiating knowledge exchange, a smart contract is executed and its outcome is written into the shared ledger. The next step is to reference the stored smart contract outcome (transaction ID) in selected knowledge exchange operations through the InterConnect SIL. The logic and granularity of the contract referencing is at the integrator's discretion. Smart contract can be executed before each knowledge exchange, or executed once for a defined period of time. With this feature the stakeholders participating in semantically interoperable ecosystems can perform the following operations:
    - Define and execute payments and other means of reimbursements for performed knowledge exchanges.
    - Organize a decentralized log of knowledge exchanges for trusted traceability of performed interactions within and between interoperable ecosystems.
    - Support reward/incentive mechanism for stakeholders to achieve higher levels of interoperability to be able to facilitate more comprehensive knowledge exchanges.

The blockchain technology of choice for the InterConnect Interoperability Framework features listed above is Hyperledger Fabric (see section 4.4 for justifications on why the project uses Hyperledger Fabric). This technology allows for full configurability of the blockchain architectures, supports privacy features (options for deleting data and establishing channels with strict access rights) and attribute-based access control. It also ensures high performance (fast) transaction executions and minimizes the power consumption overhead of public permissionless blockchains which rely on proof of work consensus methods.

4.7 SUPPORTING ENABLERS AND INTEROPERABILITY FRAMEWORK SERVICES

Apart from the main enablers, the InterConnect Interoperability Framework will include supporting enablers for production grade system operation. This subsection provides an overview of system performance monitoring, cloud services supporting hosting and tools supporting developers and system integrators.

4.7.1 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 consider the following performance metrics[18] (list not exhaustive):

- **Service metrics** – service uptime, service response speed/rate, service error responses;
- **Platform metrics** – platform uptime, platform 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.

4.7.2 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 actively managed with proper development and organization of the Interoperability Framework enablers. Other supporting enablers for cloud-based hosting will be identified and documented during WP5.

4.7.3 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 for all interoperability enablers** with detailed instructions on how to configure/instantiate a software component;
- **Project Wiki page** for all technical documentation for all Interoperability Framework enablers[19].
- **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 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.

[18] Metrics are criteria to compare the performances of a system. In general, the metrics are related to speed, accuracy, reliability, and availability of services.

[19] https://gitlab.inesctec.pt/groups/interconnect-public/-/wikis/home

5. PILOT'S IMPLEMENTATION STRATEGY

This section introduces a bird's eye view of each of the pilot maps[20], depicting the role for the Interoperability Framework and the Generic Interoperability Adapters as the interoperable link of service capabilities and data. The flexible and distributed design of the Interoperability Framework allows it to be deployed under distinct configurations, catering for the heterogeneity of the pilots, enabling at the same time the reuse of key components. The goal of each pilot is to utilize the Interoperability Framework to create semantically interoperable ecosystems comprising digital platforms, services and devices provided by the participating stakeholders (see Figure 33 for illustration). Each pilot and stakeholder can choose which interoperable resources will be provided to the parties outside of the pilot's ecosystem. This opens possibilities for establishing cross pilot interoperable ecosystems focused on a specific use case or service.

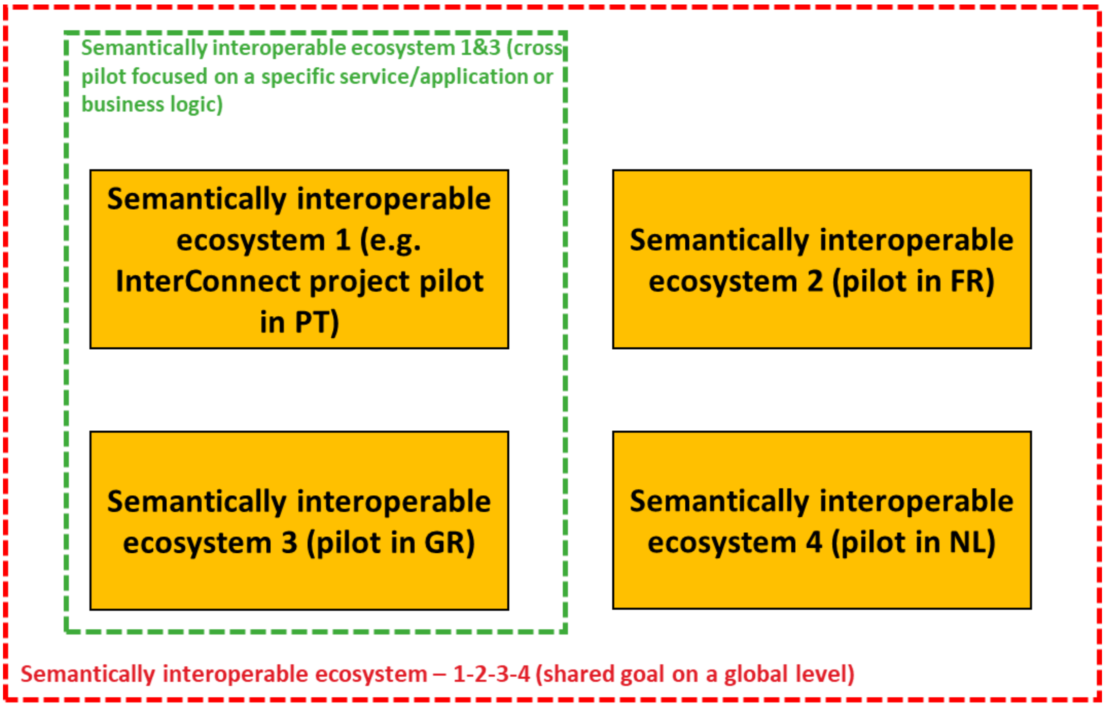
Semantically interoperable ecosystem 1&3 (cross pilot focused on a specific service/application or business logic)
Semantically interoperable ecosystem 1 (e.g. InterConnect project pilot in PT)
Semantically interoperable ecosystem 2 (pilot in FR)
Semantically interoperable ecosystem 3 (pilot in GR)
Semantically interoperable ecosystem 4 (pilot in NL)
Semantically interoperable ecosystem – 1-2-3-4 (shared goal on a global level)

FIGURE 33 - INTEROPERABILTIY FRAMEWORK SUPPORTS ESTABLISHEMNT OF SEMANTICALLY INTEROPERABLE ECOSYSTEMS

There are seven pilots within the InterConnect project, based in seven countries: Belgium, France, Greece, Germany, Italy, Portugal, and the Netherlands. While some pilots deploy several sub-pilots, only one representation per pilot is considered in this section. Moreover, an overarching pilot will show the uptake of the project's results in a cross-pilot deployment that will interoperate with other pilots. More details on each pilot can be found in the Annex 2 to this document.

THE INTERCONNECT INTEROPERABILITY FRAMEWORK FOR BUILDING SEMANTICALLY INTEROPERABLE ECOSYSTEMS IN PILOTS

The InterConnect Interoperability Framework enables syntactic and semantic interoperability between digital systems comprising semantically interoperable ecosystems (see Figure 34). It provides different means for instantiation from centrally hosted facilitator (used for proof of concept integrations and validations) to distributed framework maintained by interoperable ecosystem stakeholders. The Framework components can be instantiated on different system layers (from devices to public clouds).

[20] The details of this questionnaire are provided in Annex 2 - Pilot's Interoperability Requirements and implementation strategy.

The Framework provides support services needed for realizing secure and scalable interoperable ecosystems. Finally, the Framework provides the basis for realizing semantically interoperable services and their interconnection into semantically interoperable ecosystems. The Framework and the semantically interoperable services enable project pilots to instantiate the project's reference architecture by interconnecting available digital systems.

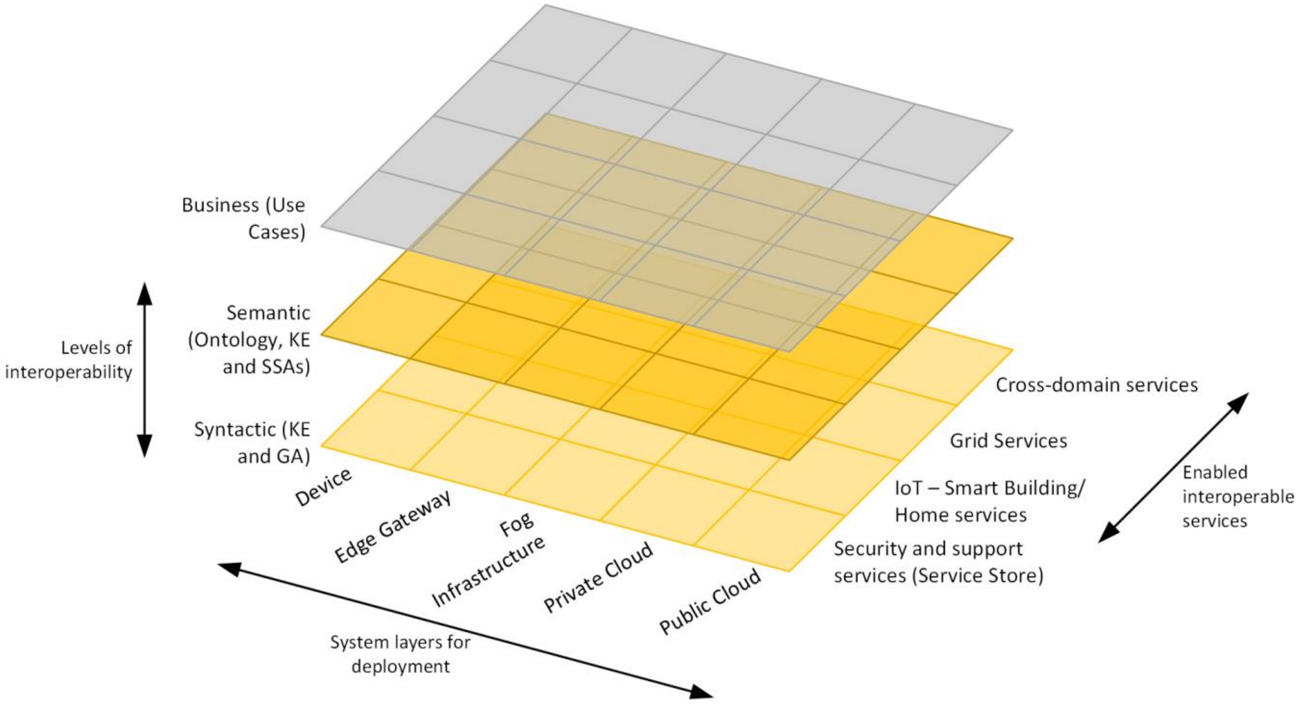
Business (Use Cases)
Semantic (Ontology, KE and SSAs)
Syntactic (KE and GA)
Levels of interoperability
Cross-domain services
Grid Services
IoT – Smart Building/ Home services
Security and support services (Service Store)
Enabled interoperable services
Device
Edge Gateway
Fog Infrastructure
Private Cloud
Public Cloud
System layers for deployment

FIGURE 34 - INTERCONNECT INTEROEPRABILITY FRAMEWORK - LEVELS OF INTEROEPRABILITY AND DEPLOYMENT OPTIONS

The WP5 initiated "interoperability workshops" with pilot teams in June 2020. The starting point was the exercise where pilots illustrated high level system architecture indicating participating digital platforms and other relevant resources and services and integration paths between them. After drafting pilot system architectures depicting participating digital platforms, actors and services, pilot teams were provided with a concept of semantic interoperability adapter which can integrate with any legacy technology. They were asked to map the interoperability adapter onto the pilot's system architecture in parts of the architecture where semantic interoperability must be achieved to support envisioned use cases. This led to specification of semantic interoperability requirements indicting:

- Which legacy technologies must be supported?
- Onto which system levels (device, edge, fog, cloud) SIL components must be deployable?
- Which interfacing technologies must be addressed?
- Which business integration rules must be supported?
- Which security and privacy protection limitations must be facilitated or enhanced by the framework?

This analysis and requirement specification provided key inputs into the process of specifying requirements and then overall architecture and specific components of the Interoperability Framework.

After specification of the Interoperability Framework architecture, and initial development results, pilot team members, who are part of WP5 tasks, started working on proof-of-concept implementation and more unified planning of the framework deployment. Figure 35 presents a high-level architectural map of the InterConnect Interoperability Framework in context of the project pilots and their typical ecosystems. The figure depicts digital platforms with a set of interoperable services, which establish semantically interoperable ecosystem through an instance of the Interoperability Framework. The next exercise was to map each pilot onto this high-level depiction of a semantically interoperable ecosystem.

In the following sub-sections we present this high level mapping of the existing pilots' digital platforms, services and devices onto the Interoperability Framework ecosystem. The main goal is to showcase that the Framework enables different digital platforms (more specifically their services) from different domains and with different architecture and technology stacks to semantically interoperate and establish basis for knowledge federation and use cases based on it.

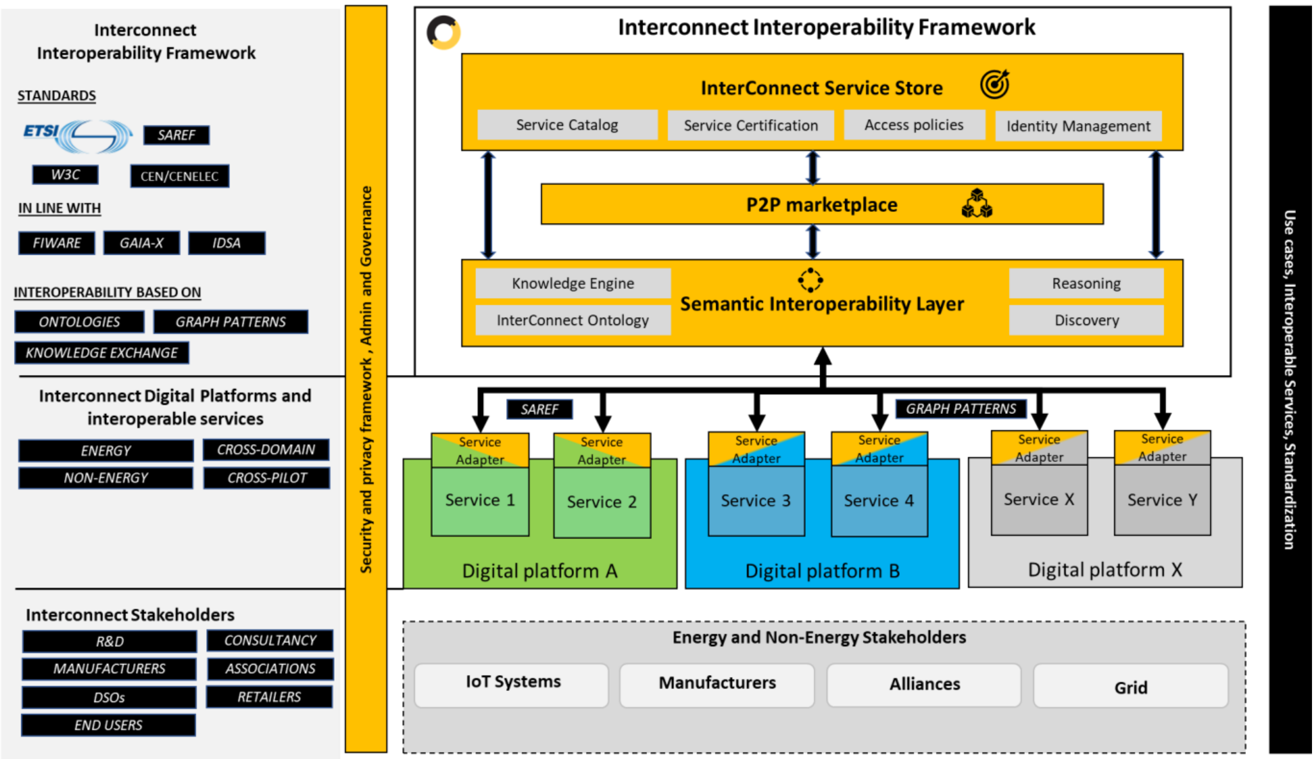

FIGURE 35 - INTERCONNECT INTEROPERABILITY FRAMEWORK AND ECOSYSTEM FOR PILOTS

Pilots Instantiation of the Architecture of the Interoperability Framework

The pilots' approach is to detail on the specific implementation aspects of interconnecting the different platforms on the field while adopting the good practices and definitions of the architecture of the Interoperability Framework.

The figures of the pilot architecture presented in the following sub-sections depict:

- Participating digital platforms provided by the pilot partners. Different colours represent the fact that most digital platforms are custom built systems with proprietary technology stacks.
- Interoperable services provided by each digital platform.
- Device management services – indicate that platform directly engages with the devices. Platforms that feature this type of service will host the SSAs built for the manufacturers represented in the project so that the same appliances can be utilized in any project pilot.
- List of devices that the pilot deploys in the field.

The figures are a preliminary work on presenting each pilots' architecture in a unified way. Refinements of the mappings are possible and expected as the pilots proceed with deployment and integration of the Interoperability Framework. Mapping of the pilot ecosystems to the InterConnect reference architecture is documented in Annex 6 of D2.1 [12].

5.1 FRENCH PILOT

The French pilot architecture, depicted in Figure 36, with a cloud and home/municipality dimension. The former realizes the InterConnect Interoperability Framework, considering several Adapters to connect and enable services with semantic data exchange capabilities. The latter addresses field installations where devices and intermediate systems interact with the cloud dimension of the pilot. The pilot comprises five digital platforms each providing a specific set of interoperable services. The pilot will deploy SIL among the participating digital platforms and work on configurations which guarantee that the selected semantically interoperable services from the French pilot can be used by other pilots. The goal is also to explore possibilities to utilize semantically interoperable services from other pilots in the scope of French pilot use cases. The Interoperability Framework setup fully supports this strategy. Finally, the pilot will employ the DSO interface services (as specified in WP4) as part of integration with the ENEDIS services.

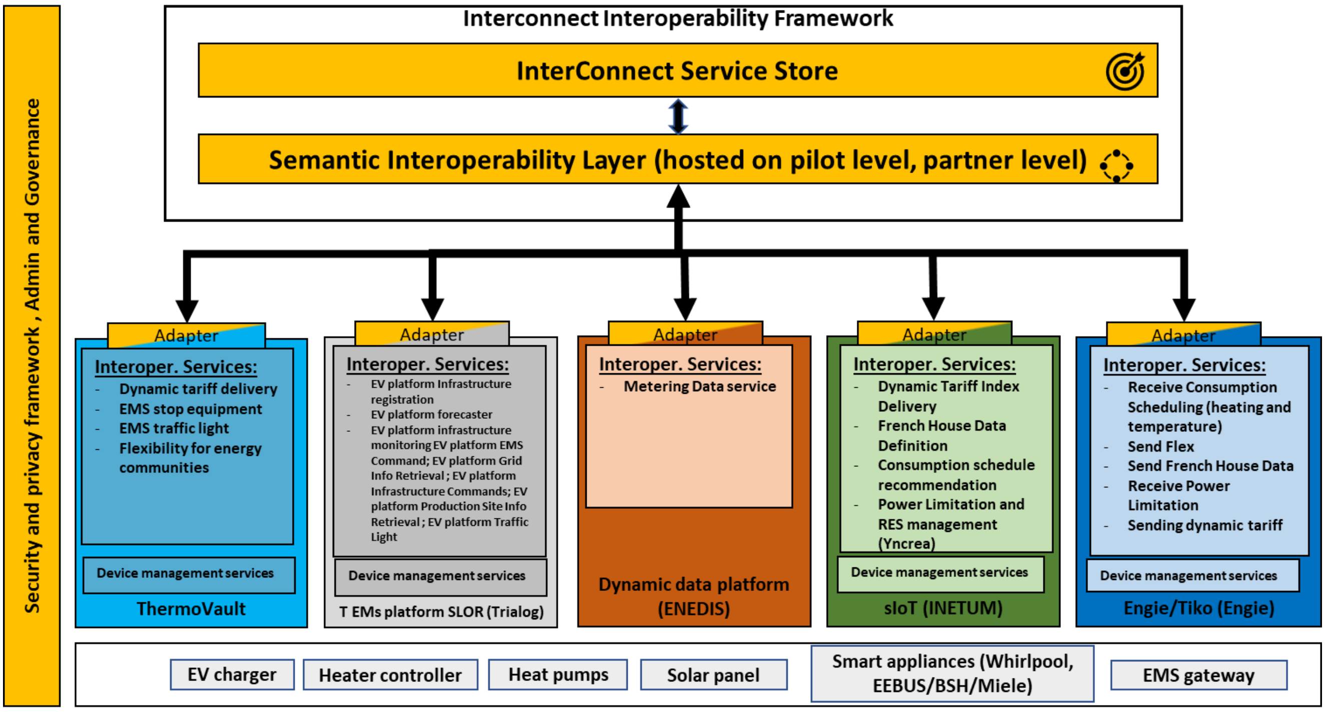
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
Semantic Interoperability Layer (hosted on pilot level, partner level)
Adapter
Interoper. Services:
- Dynamic tariff delivery
- EMS stop equipment
- EMS traffic light
- Flexibility for energy communities
Device management services
ThermoVault
Adapter
Interoper. Services:
- EV platform Infrastructure registration
- EV platform forecaster
- EV platform infrastructure monitoring EV platform EMS Command; EV platform Grid Info Retrieval ; EV platform Infrastructure Commands; EV platform Production Site Info Retrieval ; EV platform Traffic Light
Device management services
T EMs platform SLOR (Trialog)
Adapter
Interoper. Services:
- Metering Data service
Dynamic data platform (ENEDIS)
Adapter
Interoper. Services:
- Dynamic Tariff Index Delivery
- French House Data Definition
- Consumption schedule recommendation
- Power Limitation and RES management (Yncrea)
Device management services
sIoT (INETUM)
Adapter
Interoper. Services:
- Receive Consumption Scheduling (heating and temperature)
- Send Flex
- Send French House Data
- Receive Power Limitation
- Sending dynamic tariff
Device management services
Engie/Tiko (Engie)
EV charger
Heater controller
Heat pumps
Solar panel
Smart appliances (Whirlpool, EEBUS/BSH/Miele)
EMS gateway

FIGURE 36 - FRENCH PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.2 BELGIAN PILOT

The Belgium pilot is composed of 7 sub-pilot instantiations. Figure 37 depicts the 5 main participating digital platforms and also indicates that two sub-pilots focus on deploying P2P marketplace enablers for realization of smart community energy trading use cases. Each digital platform presented in the figure corresponds to a specific sub-pilot. Each digital platform will host its instance of the SIL making the pilot's integration of the Interoperability Framework completely distributed. The Belgian sub-pilots are working on enabling a full-service reuse (thanks to semantic interoperability) within the Belgian ecosystem as well as providing semantically interoperable services to other pilots.

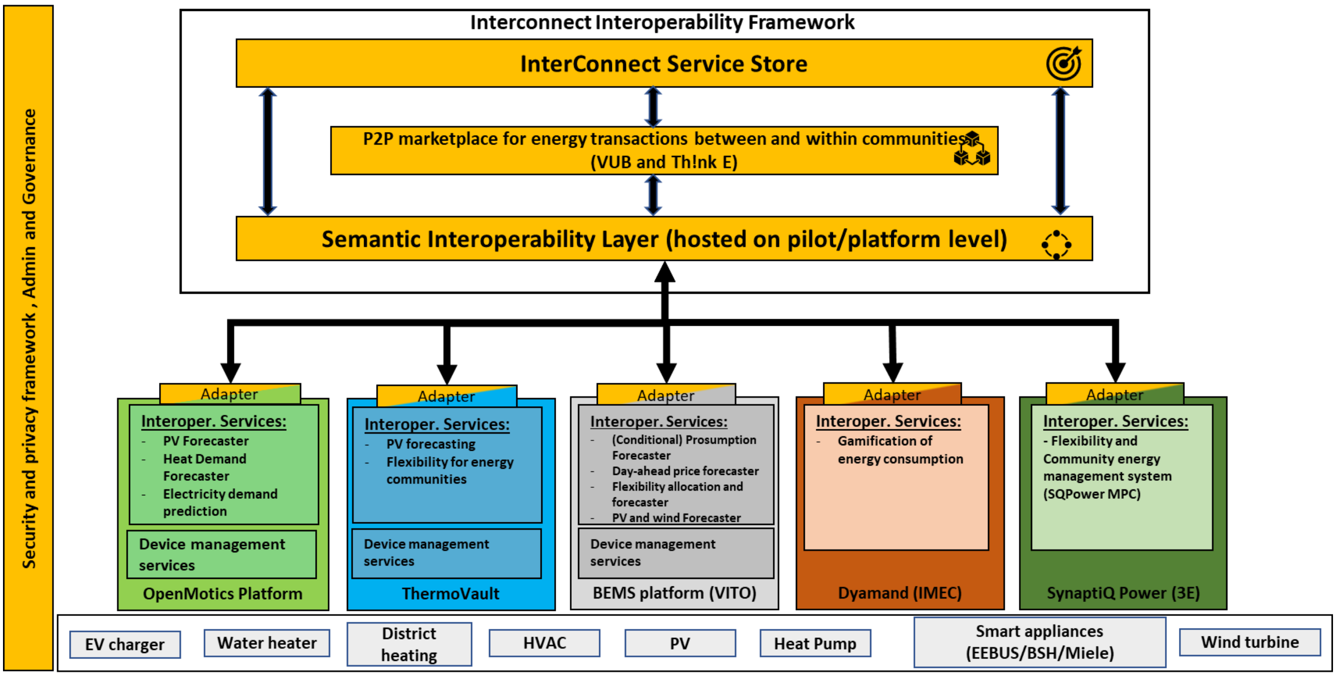
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
P2P marketplace for energy transactions between and within communities
(VUB and Th!nk E)
Semantic Interoperability Layer (hosted on pilot/platform level)
Adapter
Interoper. Services:
- PV Forecaster
- Heat Demand Forecaster
- Electricity demand prediction
Device management services
OpenMotics Platform
Adapter
Interoper. Services:
- PV forecasting
- Flexibility for energy communities
Device management services
ThermoVault
Adapter
Interoper. Services:
- (Conditional) Prosumption Forecaster
- Day-ahead price forecaster
- Flexibility allocation and forecaster
- PV and wind Forecaster
Device management services
BEMS platform (VITO)
Adapter
Interoper. Services:
- Gamification of energy consumption
Dyamand (IMEC)
Adapter
Interoper. Services:
- Flexibility and Community energy management system (SQPower MPC)
SynaptiQ Power (3E)
EV charger
Water heater
District heating
HVAC
PV
Heat Pump
Smart appliances (EEBUS/BSH/Miele)
Wind turbine

FIGURE 37 - BELGIAN PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.3 GREEK PILOT

The Greek pilot architecture is depicted in Figure 38 and it comprises 6 digital platforms. Four platforms directly interact with the devices and two focus on providing interoperable services acting on federated knowledge pools. Three platforms feature the same semantically interoperable services, but tailored for specific devices that the platforms integrate with. Also, the pilot features specific cross-platform user authorization which will be supported by the Interoperability Framework. The pilot will deploy one SIL instance on the pilot level to be shared among participating stakeholders. The pilot plans to provide semantically interoperable services to other pilots (including the cross-pilot use case) and plans to test usage of semantically interoperable services from other pilots as the use cases evolve.

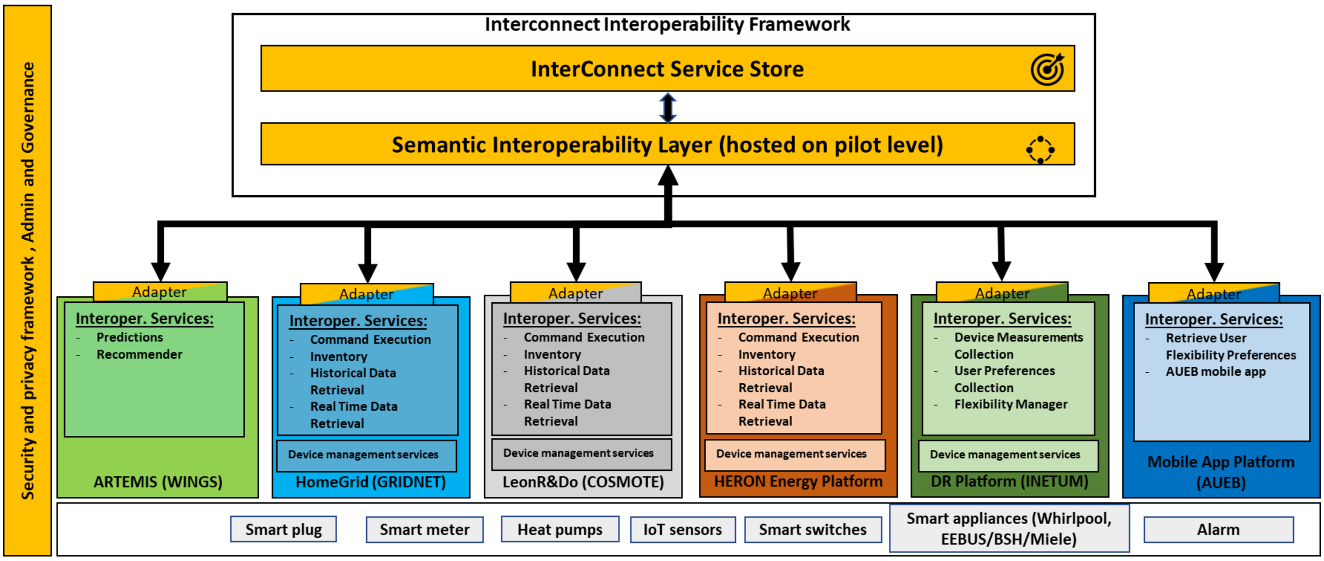
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
Semantic Interoperability Layer (hosted on pilot level)
Adapter
Interoper. Services:
- Predictions
- Recommender
ARTEMIS (WINGS)
Adapter
Interoper. Services:
- Command Execution
- Inventory
- Historical Data Retrieval
- Real Time Data Retrieval
Device management services
HomeGrid (GRIDNET)
Adapter
Interoper. Services:
- Command Execution
- Inventory
- Historical Data Retrieval
- Real Time Data Retrieval
Device management services
LeonR&Do (COSMOTE)
Adapter
Interoper. Services:
- Command Execution
- Inventory
- Historical Data Retrieval
- Real Time Data Retrieval
Device management services
HERON Energy Platform
Adapter
Interoper. Services:
- Device Measurements Collection
- User Preferences Collection
- Flexibility Manager
Device management services
DR Platform (INETUM)
Adapter
Interoper. Services:
- Retrieve User Flexibility Preferences
- AUEB mobile app
Mobile App Platform (AUEB)
Smart plug
Smart meter
Heat pumps
IoT sensors
Smart switches
Smart appliances (Whirlpool, EEBUS/BSH/Miele)
Alarm

FIGURE 38 - GREEK PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.4 PORTUGUESE PILOT

The Portuguese pilot architecture is depicted in Figure 39. This pilot considers two logical dimensions, namely a Commercial and Residential. Both are comprehended by a series of services and intermediate middleware systems that connect to a group of digital platforms. The pilot comprises 6 digital platforms with specific services offered within and between commercial and residential use cases. DSO interface plays important role in this pilot as E-REDES is the lead partner. The pilot will deploy SIL on the pilot level and on specific digital platforms for finer granularity of configurations for knowledge federation. The Portuguese pilot also considers the P2P marketplace enablers of the Interoperability Framework within the scope of the residential demonstration for user profile sharing and flexibility aggregation.

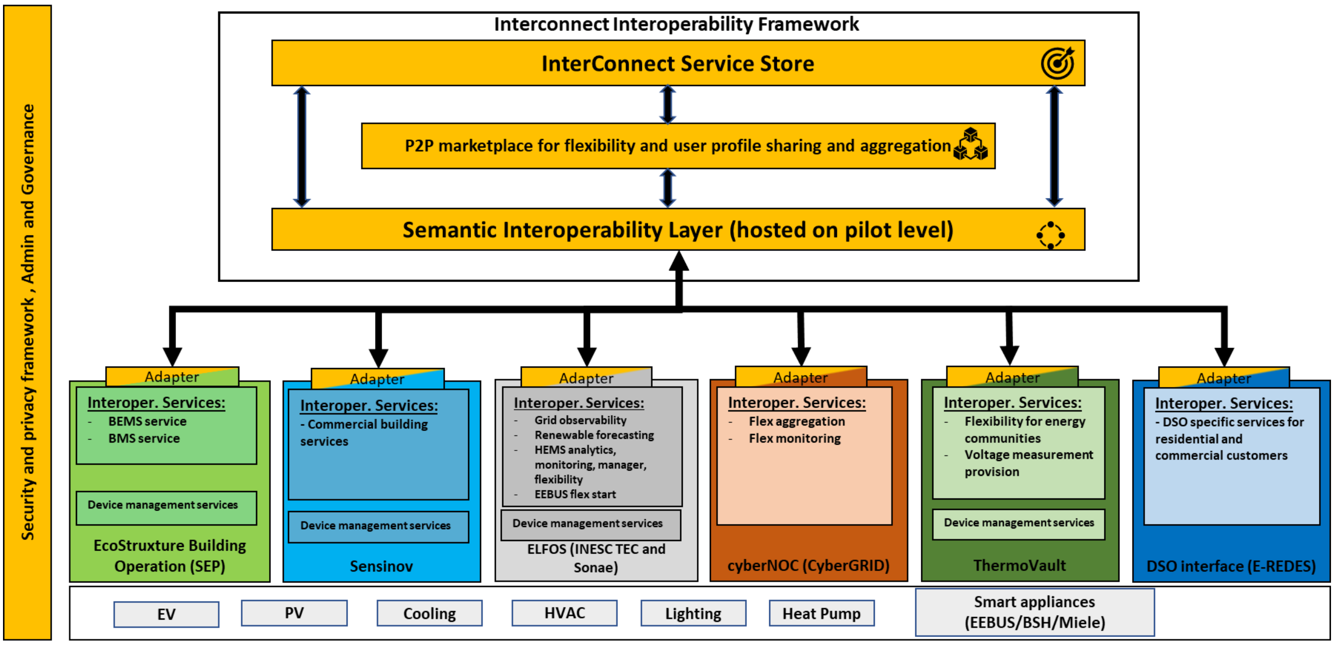
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
P2P marketplace for flexibility and user profile sharing and aggregation
Semantic Interoperability Layer (hosted on pilot level)
Adapter
Interoper. Services:
- BEMS service
- BMS service
Device management services
EcoStruxture Building Operation (SEP)
Adapter
Interoper. Services:
- Commercial building services
Device management services
Sensinov
Adapter
Interoper. Services:
- Grid observability
- Renewable forecasting
- HEMS analytics, monitoring, manager, flexibility
- EEBUS flex start
Device management services
ELFOS (INESC TEC and Sonae)
Adapter
Interoper. Services:
- Flex aggregation
- Flex monitoring
cyberNOC (CyberGRID)
Adapter
Interoper. Services:
- Flexibility for energy communities
- Voltage measurement provision
Device management services
ThermoVault
Adapter
Interoper. Services:
- DSO specific services for residential and commercial customers
DSO interface (E-REDES)
EV
PV
Cooling
HVAC
Lighting
Heat Pump
Smart appliances (EEBUS/BSH/Miele)

FIGURE 39 - PORTUGUESE PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.5 GERMAN PILOT

The German pilot is composed by 2 sub-pilot instantiations. Figure 40 depicts the Hamburg location sub-pilot. The SIL will be deployed on the pilot level and shared among two digital platforms. There are two additional digital platforms which will be integrated on a syntactic level. The EEBUS German pilot will provide an instantiation for SPINE enabled devices along with the respective SAREF translation. The EEBUS/SPINE SSA will be reused in most other project pilots.

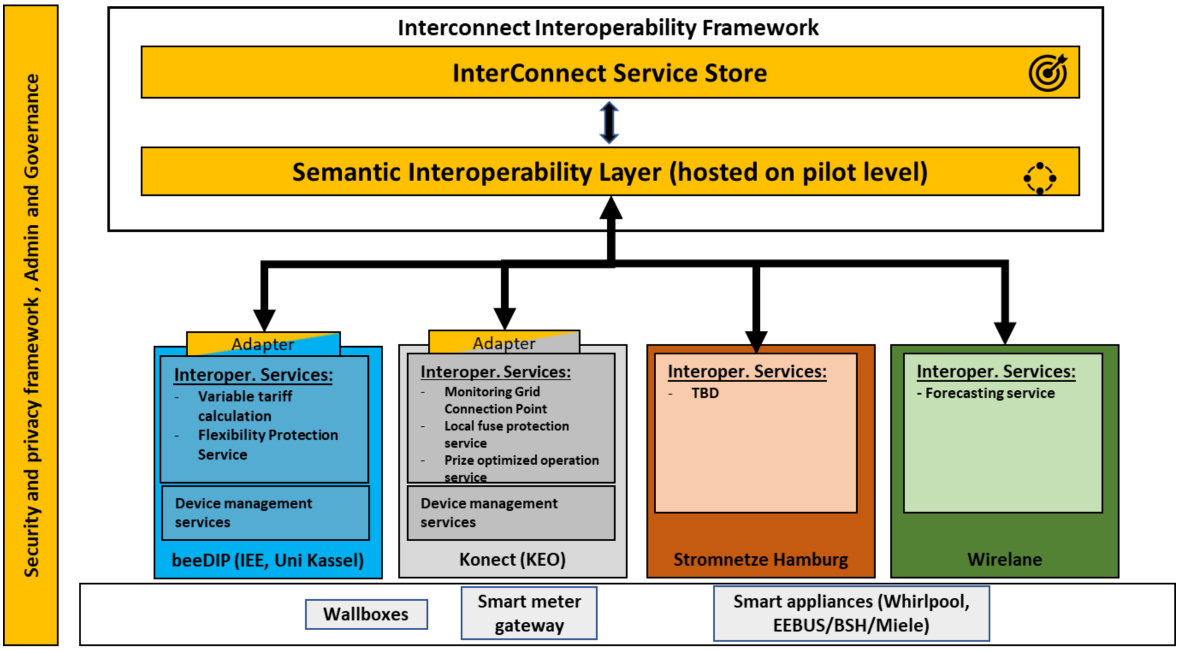
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
Semantic Interoperability Layer (hosted on pilot level)
Adapter
Interoper. Services:
- Variable tariff calculation
- Flexibility Protection Service
Device management services
beeDIP (IEE, Uni Kassel)
Adapter
Interoper. Services:
- Monitoring Grid Connection Point
- Local fuse protection service
- Prize optimized operation service
Device management services
Konect (KEO)
Interoper. Services:
- TBD
Stromnetze Hamburg
Interoper. Services:
- Forecasting service
Wirelane
Wallboxes
Smart meter gateway
Smart appliances (Whirlpool, EEBUS/BSH/Miele)

FIGURE 40 - GERMAN HAMBURG SUB-PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.6 DUTCH PILOT

The Dutch pilot architecture is depicted in Figure 41. It comprehends two dimensions as previous pilots, namely a public cloud dimension, considering multiple digital services and, a building/apartment dimension, considering a set of residential structures where devices are managed via a local EMS capable device. The SIL will be hosted on pilot level. The pilot plans for service reusability between all other pilots. The pilot will utilize P2P marketplace enablers to setup an IoT data marketplace integrated with the Hyrde ECKO data catalogue platform.

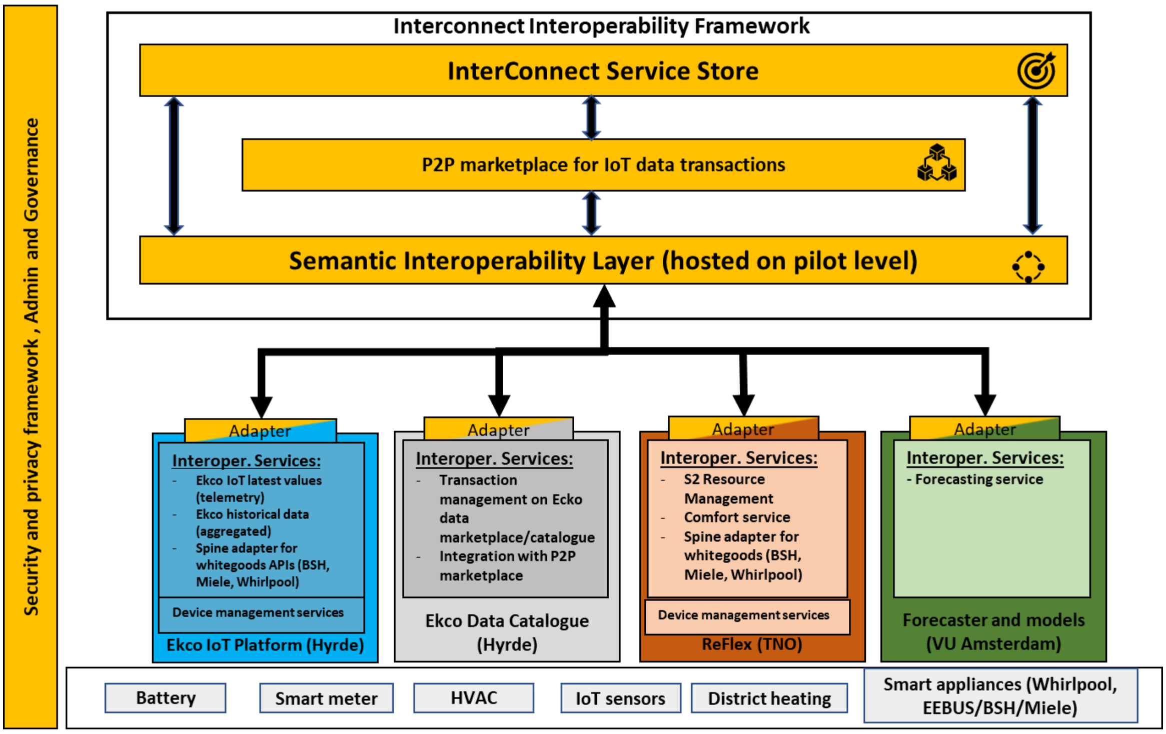
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
P2P marketplace for IoT data transactions
Semantic Interoperability Layer (hosted on pilot level)
Adapter
Interoper. Services:
- Ekco IoT latest values (telemetry)
- Ekco historical data (aggregated)
- Spine adapter for whitegoods APIs (BSH, Miele, Whirlpool)
Device management services
Ekco IoT Platform (Hyrde)
Adapter
Interoper. Services:
- Transaction management on Ecko data marketplace/catalogue
- Integration with P2P marketplace
Ekco Data Catalogue (Hyrde)
Adapter
Interoper. Services:
- S2 Resource Management
- Comfort service
- Spine adapter for whitegoods (BSH, Miele, Whirlpool)
Device management services
ReFlex (TNO)
Adapter
Interoper. Services:
- Forecasting service
Forecaster and models (VU Amsterdam)
Battery
Smart meter
HVAC
IoT sensors
District heating
Smart appliances (Whirlpool, EEBUS/BSH/Miele)

FIGURE 41 - DUTCH PILOT SEMANTICALLY INTEROEPRABLE ECOSYSTEM

5.7 ITALIAN PILOT

The Italian pilot architecture is depicted in Figure 42. The Planet App is the central point for hosting the SIL and supporting integration of interoperable services provided by the two other digital platforms. This pilot will also provide services for integrating Whirlpool appliances in all other projects. The Italian pilot plans for integration of services from other project pilots towards realisation of its use cases.

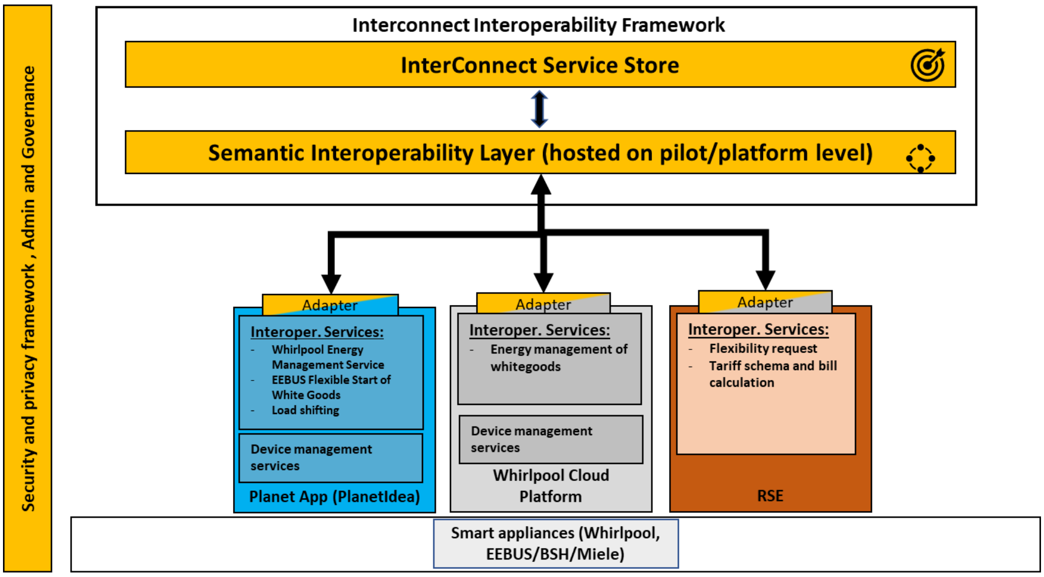
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
Semantic Interoperability Layer (hosted on pilot/platform level)
Adapter
Interoper. Services:
- Whirlpool Energy Management Service
- EEBUS Flexible Start of White Goods
- Load shifting
Device management services
Planet App (PlanetIdea)
Adapter
Interoper. Services:
- Energy management of whitegoods
Device management services
Whirlpool Cloud Platform
Adapter
Interoper. Services:
- Flexibility request
- Tariff schema and bill calculation
RSE
Smart appliances (Whirlpool, EEBUS/BSH/Miele)

FIGURE 42 - ITALIAN PILOT SEMANTICALLY INTEROPERABLE ECOSYSTEM

5.8 CROSS-PILOT DEMO FOR ANCILLARY SERVICES

The Cross-pilot architecture is depicted in Figure 43. This pilot demonstrates the individual uptake brought by individual pilots in mapping their flexibility resources in an interoperable way. The central point is the CyberNOC platform for flexibility aggregation and it will host SIL instance which will be shared with all other pilots which participate in the flexibility reporting and aggregation use case setup by this pilot. The cross-pilot approach will be expanded with the cascade funding demonstrators as well. The pilot will emulate specific services that can be offered to a wider energy market based on the managed knowledge about cross-border flexibility collected from other project pilots.

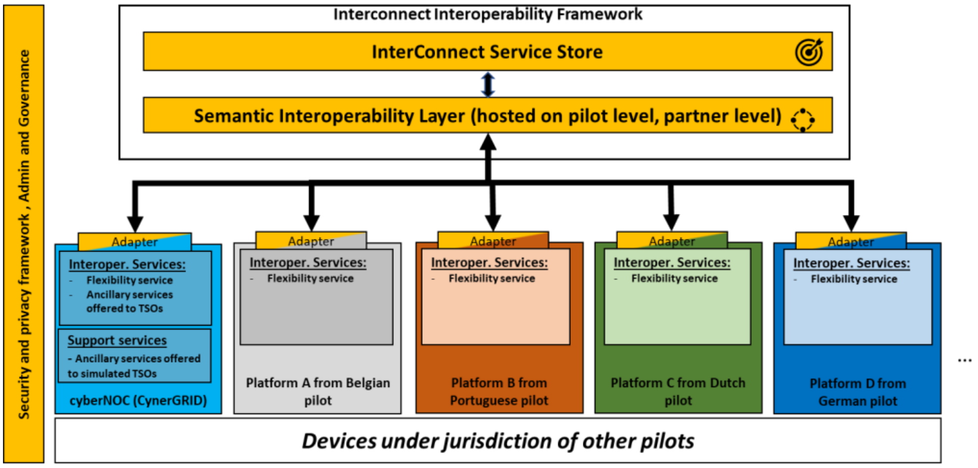
Security and privacy framework , Admin and Governance
Interconnect Interoperability Framework
InterConnect Service Store
Semantic Interoperability Layer (hosted on pilot level, partner level)
Adapter
Interoper. Services:
- Flexibility service
- Ancillary services offered to TSOs
Support services
- Ancillary services offered to simulated TSOs
cyberNOC (CynerGRID)
Adapter
Interoper. Services:
- Flexibility service
Platform A from Belgian pilot
Adapter
Interoper. Services:
- Flexibility service
Platform B from Portuguese pilot
Adapter
Interoper. Services:
- Flexibility service
Platform C from Dutch pilot
Adapter
Interoper. Services:
- Flexibility service
Platform D from German pilot
...
Devices under jurisdiction of other pilots

FIGURE 43 - CYBERGRID OVERARCHING USE CASE SEMANTICALLY INTEROPERABLE ECOSYSTEM

6. CONCLUDING REMARKS

What was the purpose of this document?

This document reports the current progress and results of the WP5 (more precisely Task 5.1) activities within the InterConnect project. The main objective of this period was to specify architecture and key enablers of the secure, trusted, and flexible semantic Interoperability Framework for the project.

How was the InterConnect Interoperability Framework specified?

Document is organized so that it depicts the actual methodology applied for analysing landscape of available solution for semantic interoperability, reference approaches and architectures, requirements/capabilities/limitations of the digital platforms brought to the project by the partners and finally interoperability requirements for building semantically interoperable ecosystems representing the project pilots. All this led to derivation of the high-level requirements and, finally, specification of the InterConnect Interoperability Framework architecture.

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 **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 T5.2 *"Implementation of the interoperability toolbox and service store*" development and integration activities per digital platform and per IC Interoperability Framework enabler are specified.

Finally, all project pilots defined their approaches for establishing semantically interoperable ecosystems utilizing the InterConnect Interoperability Framework. This exercise led to refinement of the requirements and set certain technical and organizational limitations to the concept of semantic interoperability that needs to be achieved by the presented Interoperability Framework.

What are the main components of the presented Interoperability Framework architecture?

The main components of the InterConnect Interoperability Framework are:

- Details about the IC semantic interoperability layer (SIL) are presented. The main SIL components are presented in detail. This specification of the Knowledge Engine, generic Adapter and Service Specific Adapter are result of the actual development and integration work that happened in the cope of T5.2. We have decided to include this additional information into D5.1 so that the document is up to date with the project status at the moment of deliverable publication.
- The IC service store is presented as the main catalogue of all interoperable energy and non-energy services. It is also the main identity provider for services and users.
- 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 InterConnect security and data protection framework is introduced. The main innovation pursued by the project relates to integration of authorization, access control and privacy protection mechanisms with the semantic interoperability layer.

One of the guiding requirements in specifying and implementing the Interoperability Framework was to enable semantic interoperability without a centrally hosted facilitator. The Interoperability Framework has one centrally hosted component, the Service Store. It is implemented and hosted centrally on the project level because it is a frontend of the Framework and provides single stop for pilots, integrators and users to get familiar with the interoperable ecosystem of the project. It is also a centralized identity manager. The SIL (and Knowledge Engine) can and is also hosted centrally on the project level, but that is mainly for testing purposes and in support of proof-of-concept integrations. This centrally hosted SIL eases debugging and testing procedures. The pilots are instructed to pursue distributed deployment of the SIL in their interoperable ecosystems. This means that parts of the pilot level SIL will be centralized, but only on a pilot level and based on deployment decisions from the pilot stakeholders. A fully decentralized deployment where every digital platform from the pilots host their own Knowledge Engine Runtime and Knowledge Directory is recommended for production ready systems.

What are the plans for implementing and validating the Interoperability Framework?

The specification of the Interoperability Framework and requirements set by the digital platform providers and project pilots are inputs for the framework development and integration cycle performed within Task 5.2. The security and privacy protection framework were defined in Task 5.3 with a set of detailed security and privacy protection plans for the Interoperability Framework and the project pilots. The P2P marketplace enablers were implemented in Task 5.4. These three tasks lead towards the first complete implementation of the InterConnect Interoperability Framework.

The Interoperability Framework was supplied to the project pilots in October 2021. Key partners from the pilots (digital platform providers) were testing the Framework components since April 2021 as part of the early adopter program – agile development and validation method applied in the scope of WP5. Three workshops are organized for early adopters (individual integrators) and complete pilot teams. The last workshop was organized for pilots in December 2021 and during it the pilots were presenting and discussing their approaches and plans for deploying and configuring Interoperability Frameworks. Mappings of the Framework onto the pilots is depicted in section 5. The Framework was publicly released in January 2022 in support of the cascade funding programs as part of the project open calls, being set in WP8.

WP5 will continue to maintain and evolve the Interoperability Framework in the scope of T5.5 until the project ends. Feedback and validation results from the pilot and cascade funding projects will be used to enhance the framework components, fix performance issues, and introduce new functionalities for streamlining the semantic integration process.

What is the impact of the specified Interoperability Framework?

The Interoperability Framework specification and development process were motivated by a set of impact indicators defined by the European Commission and overall impact goals of the InterConnect project.

The main impact of the WP5 is specification, development and integration of the semantic Interoperability Framework which will enable the project partners and 3rd parties to achieve the required level of semantic interoperability and become part of a wider InterConnect ecosystem realized through the pilots. The semantic interoperability is one of the main enablers for cross-domain data spaces, so the potential impact is that the Interoperability framework can be considered as a best practice approach for building data spaces on technical level. The WP5 contributed to the specific project impact indicators in the following way:

- Increasing the number of energy apps/services and home devices and appliances that are connected through the Internet allowing to shift consumption according to wholesale market or grid-constraints-related price signals.
    - The InterConnect semantic Interoperability Framework streamlines onboarding of legacy technologies and systems into the InterConnect project ecosystem. Interoperable systems can benefit from semantic discovery, orchestration and other semantic reasoning features in order to achieve highest levels of automation, energy efficiency, comfort and convenience.
- Accelerated wider deployment and adoption of IoT standards and platforms in smart homes and buildings in Europe and development of secure, cost-effective and sustainable European IoT ecosystems and related business models.
    - The semantic Interoperability Framework of the InterConnect project is based on lessons learned from the European IoT platform initiative projects. The overall architecture is based on a set of IoT and smart grid architectural standards and references as documented in D2.1 [12]. The semantic interoperability layer is based on SAREF family of ontologies.
- Demonstration that such platforms lead to a marketplace for new services in EU homes and buildings with opportunities also for SMEs and start-ups.
    - Interoperability Framework includes InterConnect service store as a complete catalogue of all interoperable services and other endpoints. The interoperable digital platforms and applications will be able to interoperate with any interoperable service and platform to achieve specific goals. Introducing new interoperable digital systems will be streamlined with the Interoperability Framework so the project ensures that the semantically interoperable ecosystem continuously grow during and after the project runtime.
- Contribution to increasing the use of renewable energy and increased energy efficiency, offering access to cheaper and sustainable energy for consumers and maximizing social welfare.
    - The semantic Interoperability Framework opens new possibilities for developing innovative services and processes for flexibility management, forecasting and energy trading (e.g., P2P energy trading) leading to new business models and opportunities to make renewable energy management more efficient.

How will the Interoperability Framework be utilized within the project?

The Interoperability Framework components were supplied to the project pilots in October 2021. The WP5 is now in a mode of continuous support for realization of semantically interoperable ecosystems represented by the pilots. Access to the framework components will be provided through project website, and InterConnect wiki pages. Support/administration dashboard and tools are provided through the Service Store (KE Admin UI, knowledge explorers, KPI monitoring dashboard, service onboarding, compliance checks, certification, sandbox for Docker-ized services).

Documentation and source code of the released Interoperability Framework is provided through the project GitLab public repositories. This public release on January 2022 was accompanied with:

- Release documentation and deployment/configuration instructions.
- Examples and best practices prepared by partners.

- Wiki Pages[21] on GitLab and project website.
- Training webinars and workshops for project pilots and planed workshops for cascade funding partners.

It is worth noting that key partners from each project pilot also participated in the specification, development and testing of the Interoperability Framework as part of the WP5.

The lessons learned from the earl adopters and the project pilots are translated into refined documentation and methodology for the Interoperability Framework deployment and building semantically interoperable ecosystems. This refined methodology and documentation set is available to support the cascade funding programs. The cascade funding participants will get familiar with the complete Interoperability Framework during preparation of their proposals. The WP5 will provide full support for later integration of the new project extensions.

The continuous Interoperability Framework maintenance and enhancement cycles will be supported with the feedback collection mechanism as depicted in Figure 44. This figure also depicts how the Interoperability Framework as one of projects KERs will provide basis for most of the standardization and impact creation efforts of the consortium.

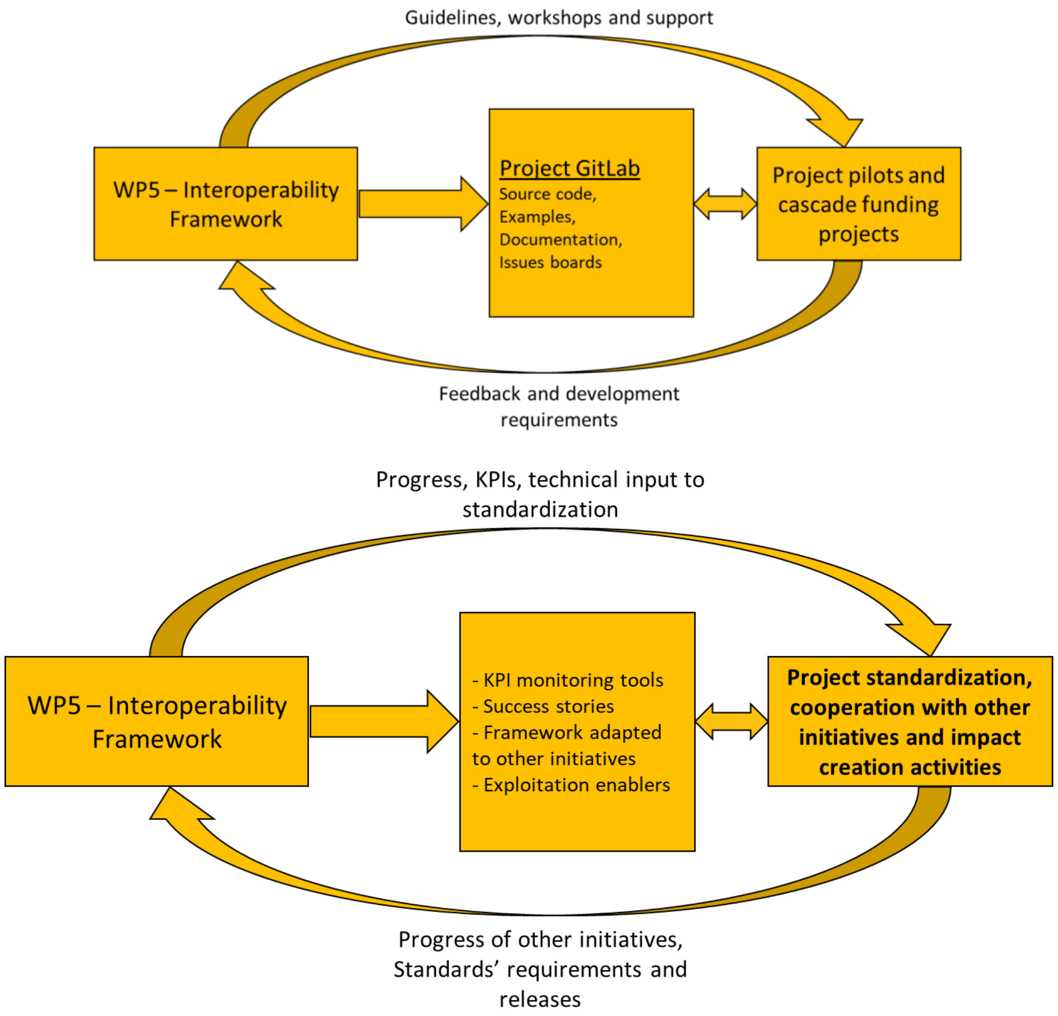
Guidelines, workshops and support
WP5 – Interoperability Framework
Project GitLab
Source code,
Examples,
Documentation,
Issues boards
Project pilots and cascade funding projects
Feedback and development requirements
Progress, KPIs, technical input to standardization
WP5 – Interoperability Framework
- KPI monitoring tools
- Success stories
- Framework adapted to other initiatives
- Exploitation enablers
Project standardization, cooperation with other initiatives and impact creation activities
Progress of other initiatives, Standards' requirements and releases

FIGURE 44 - CONTINUOUS IMPROVEMENT LOOP OF THE INTEROPERABILITY FRAMEWORK WITH THE PROJECT PILOTS AND CASCADE FUNDING; INTEROPERABILITY FRAMEWORK AS KEY EXPLOITABLE RESULT IMPACTING PROJECTS STANDARDIZATION AND IMPACT CREATION ACTIVITIES

[21] https://gitlab.inesctec.pt/groups/interconnect-public/-/wikis/home

How will wider public benefit from the Interoperability Framework?

The Interoperability Framework at this stage of development is targeting system integrators, service providers, device manufactures, application developers and digital platform operators to help them achieve semantic interoperability in a cost-effective manner while unlocking the full potential of federated knowledge pools. The Interoperability Framework was publicly released in January 2022 with continuous validation and updates afterward. All software artifacts are available for download and instantiation so that a completely independent interoperability ecosystem can be built by interested parties. Project partners are documenting their success stories and getting ready to provide their interoperability adapters as example implementations and best practices to be followed by integrators who base their systems on the same/similar technologies - learn and do by example approach that benefits from the project's consortium diversity. This is the key for ensuring the Framework uptake in the cascade funding project extensions.

Interoperable ecosystems established with instances of the Interoperability Framework will be able to run innovative value-added services targeted towards key stakeholders from IoT and energy domains including end users. Pervasive deployment of the Interoperability Framework will create a building/community/city/region/Europe-wide semantically interoperable ecosystems where devices and home management systems will be able to automatically or on demand choose among plethora of interoperable services specifically tailored for a challenge at hand. Home and building management systems will be able to aggregate and offer valuable data (e.g., demand side flexibility) to the energy marketplace decision makers. Energy communities will be able to operate without 3rd party facilitators and federate with other communities and large prosumers to improve their competitiveness on a wider energy market.

Finally, the InterConnect Interoperability Framework is defined to be ontology agnostic, so it is applicable to other domains as well, not just IoT and energy. This opens possibilities for new cross domain challenges. During the project, SAREF based semantic interoperability will be demonstrated and the framework will have a set of tools specifically tailored to SAREF.

As part of the BRIDGE initiative, the project will promote Interoperability Framework as a toolset for establishing new and bridging existing interoperable ecosystems.

Interoperability Framework development is in line with Gaia-X specifications: 1. "The users always retain sovereignty over their data. So, what emerges is not a cloud, but a federated system that links many cloud services providers and users together." IF provides the same for service providers - distributed semantic interoperability layer where service providers maintain full control over their data; 2. "Data Spaces represent a data integration concept without a central storage. Thus, data remains at its source and is only shared when needed." Interoperability Framework is used to establish distributed data spaces (interoperable ecosystems) with federated knowledge enabled through semantic interoperability and shared SAREF ontology. The goal is to promote the Interoperability Framework to the Gaia-X initiatives as a reference technology for building cross-domain data spaces based on semantic interoperability.

As part of the Open DEI Energy, the project contributes to the WG4 with its Interoperability Framework as a facilitator for building interoperable ecosystems and as an enabler for bridging different reference architectures.

The Interoperability Framework provided by WP5 together with interoperable services provided by WP3 and semantic interoperability technologies from WP2 will provide basis for building innovative applications and business models benefiting end users of the smart building and energy systems. End users will be empowered to:

- Avoid vendor lock-in when setting up their smart home systems and processes for automation.
- Achieve energy efficiency without sacrificing comfort and convenience.

- To easily swap digital service providers, seeking the ones with the most appealing set of capabilities, privacy concerns and cost.

How do we know it will work?

Reason 1 - easing the technology uptake process will attract stakeholders to consider and test the technology and be onboarded into interoperable ecosystems. Enablers for achieving semantic interoperability are defined in a way that ensures much more manageable technology uptake and learning curve than "vanilla" semantic web solutions. This will ensure that integrators can achieve full semantic interoperability with tool sets they are mostly familiar with and with enough deployment flexibility and options that will ensure their established practices are not disrupted.

Reason 2 - once onboarded, stakeholders will be motivated to maintain the achieved semantic interoperability. The Interoperability Framework is specified so that it enables interoperable ecosystems to be established and to take full advantage of federated knowledge pools. The end result is enabling components (services, devices, digital platforms) to interact with each other without having to know each other's local native API, but purely based on the knowledge of ontologies and what ontology (category) a component belongs to (e.g. forecaster service). This means that ultimately, client applications can be written without any knowledge about the supported native APIs of a component they need to interact with. It suffices to know the by-consensus semantic description of the component/concept in the SAREF reference ontology and its extensions, and based on that any imaginable knowledge-based question can be asked without any constraint or knowledge about the actual API of the addressed component. This brings completely new dimension to service and application development and maintenance, drastically reducing the costs of integrations between software components from different stakeholders. The project consortium includes key stakeholders from IoT and energy domains. Pilots will establish large scale interoperable ecosystems. As the interoperable ecosystems are validated with innovative use cases, more stakeholders will be attracted to join them (cascade funding).

REFERENCES

EXTERNAL DOCUMENTS

[1] BIG IoT, “High Level architecture specification,” 2017.

[2] A. Gyrard, “Designing cross-domain semantic Web of things applications,” *Ubiquitous Computing,* 2015.

[3] symbIoTe, “Final Report on System Requirements and Architecture,” 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, “Semantic Models for Testbeds Interoperability and Mobility Support and Best Practices V2,” 2016.

[10] bIoTope, “D2.4 bIoTope SoS Reference Platform Specification,” 2017.

INTERCONNECT DOCUMENTS

[11] InterConnect project. “D1.1 Services and use cases for smart buildings and grids”. 2021.

[12] InterConnect project. “D2.1 Secure interoperable IoT smart home/building and smart energy system reference architecture”, 2021.

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

[14] InterConnect project. “D5.3 Security, cyber-security and privacy protection action plan and results”. 2021.

ANNEX 1 – DIGITAL PLATFORM CATALOGUE

This annex 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.

IMPORTANT NOTE: architecture figures of digital platforms are provided at discretion of each platform operators. The architecture images do not reflect on InterConnect project's reference architecture, but present the way in which partners present their high TRL platforms.

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.

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>

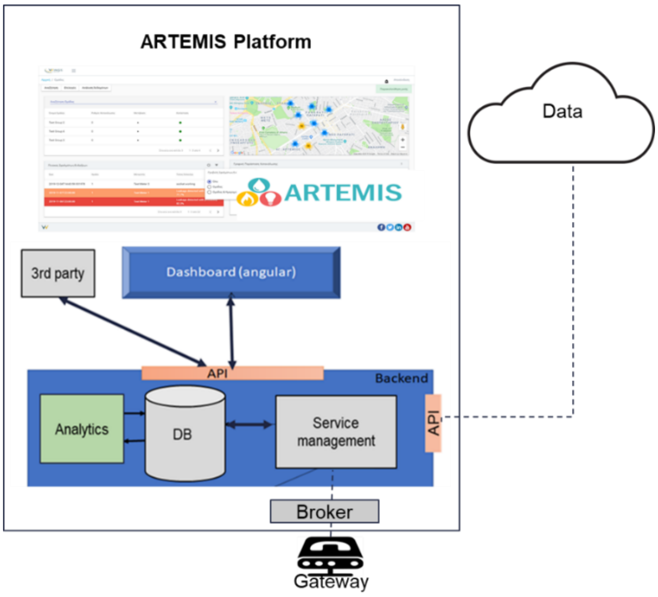

FIGURE 45 - ARTEMIS ARCHITECTURE

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.

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.

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 >

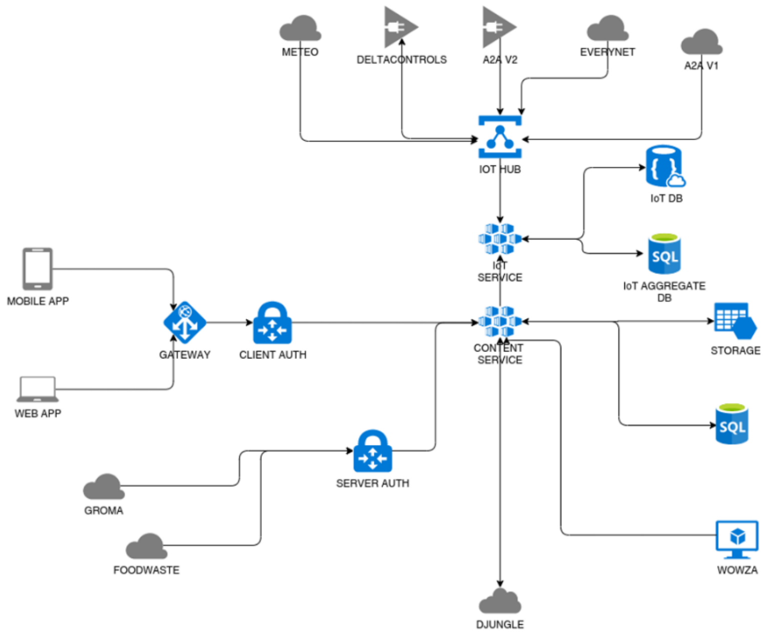

FIGURE 46 - PLANETAPP ARCHITECTURE

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

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.

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>

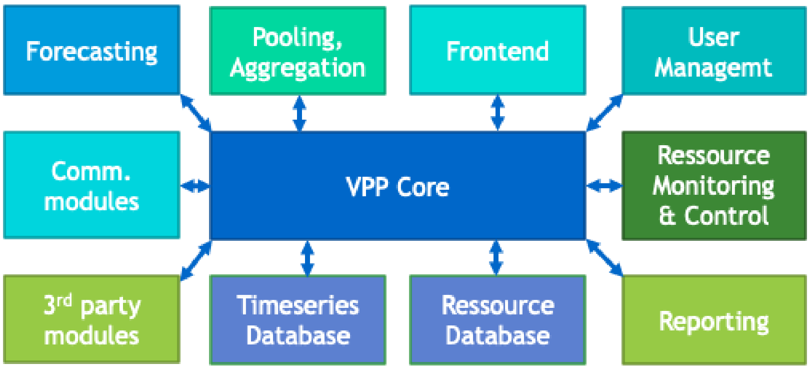

FIGURE 47 - CYBERNOC ARCHITECTURE

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

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).

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>

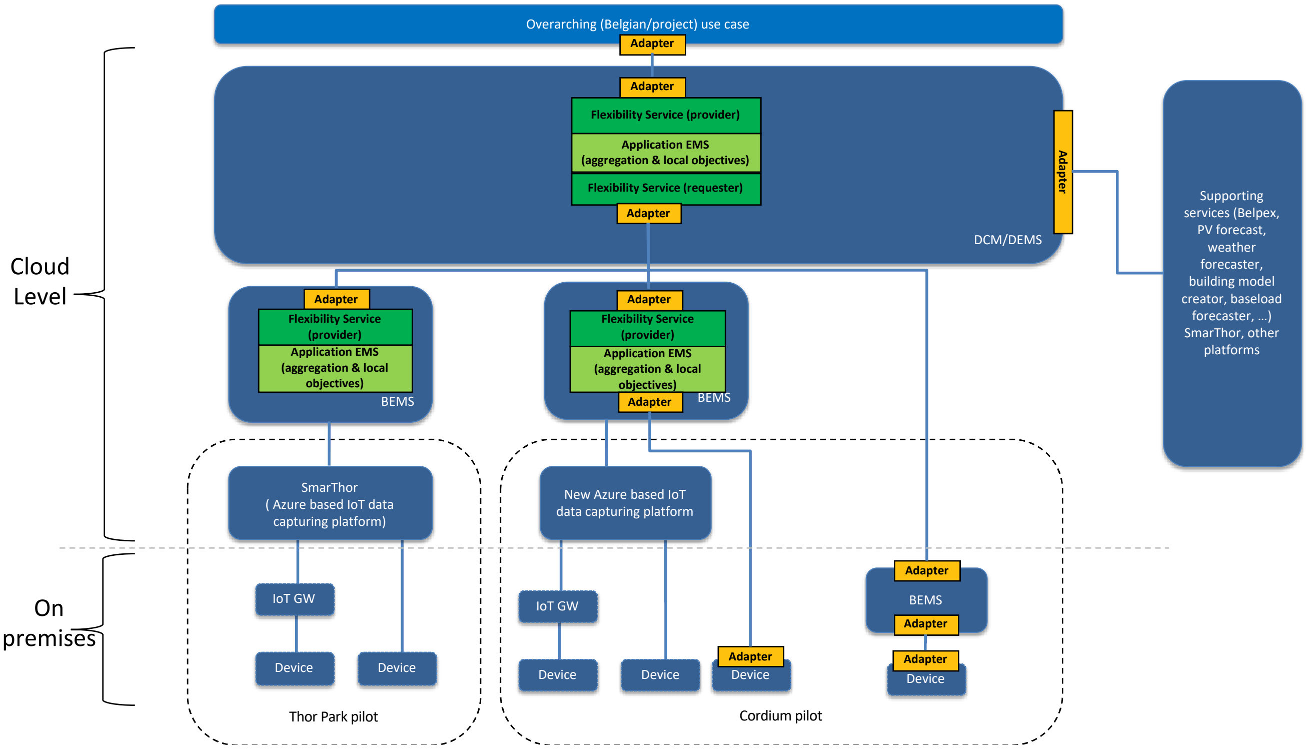
Overarching (Belgian/project) use case
Adapter
Adapter
Flexibility Service (provider)
Application EMS (aggregation & local objectives)
Flexibility Service (requester)
Adapter
Adapter
DCM/DEMS
Supporting services (Belpex, PV forecast, weather forecaster, building model creator, baseload forecaster, …) SmarThor, other platforms
Cloud Level
Adapter
Flexibility Service (provider)
Application EMS (aggregation & local objectives)
BEMS
Adapter
Flexibility Service (provider)
Application EMS (aggregation & local objectives)
Adapter
BEMS
SmarThor (Azure based IoT data capturing platform)
New Azure based IoT data capturing platform
On premises
IoT GW
Device
Device
Thor Park pilot
IoT GW
Device
Device
Adapter
Device
Adapter
BEMS
Adapter
Adapter
Device
Cordium pilot

FIGURE 48 - DCM ARCHITECTURE

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.

VITO BEMS

The Building Energy Management System from Vito will be redesigned, considering 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.

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>

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

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.

OVERVIEW

Platform name:
beeDIP
Partner:
University Kassel, IEE
Services:
Data integration
Website:
cloud.openmotics.com

Domain of operation:
<energy>
Technology readiness level
<TRL 7>

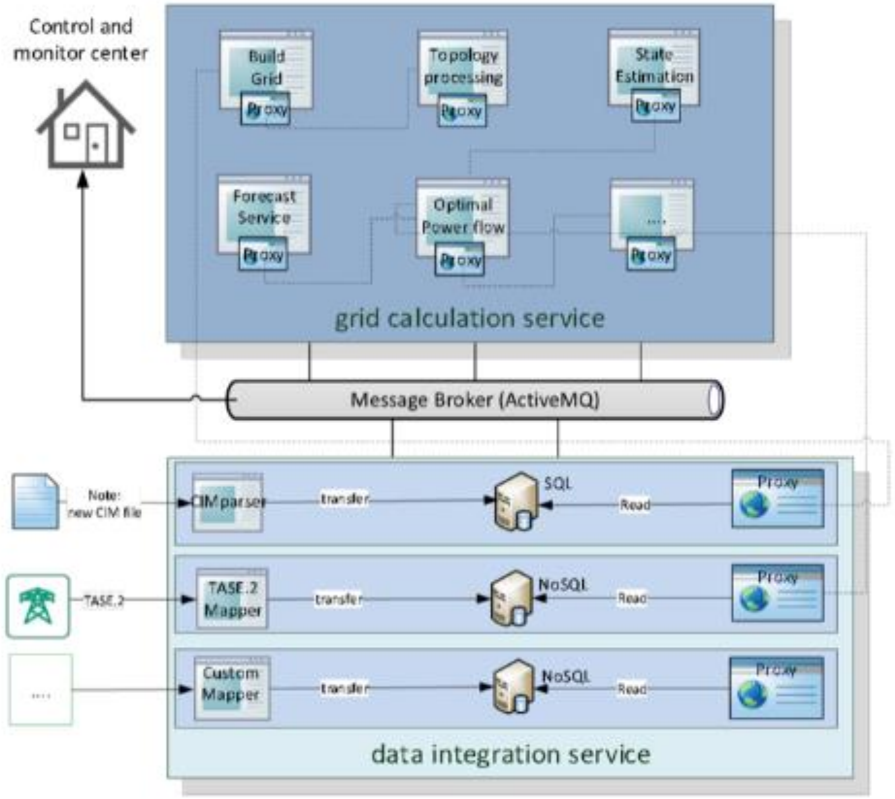

FIGURE 49 - BEEDIP ARCHITECTURE

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

S-LOR

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.

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>

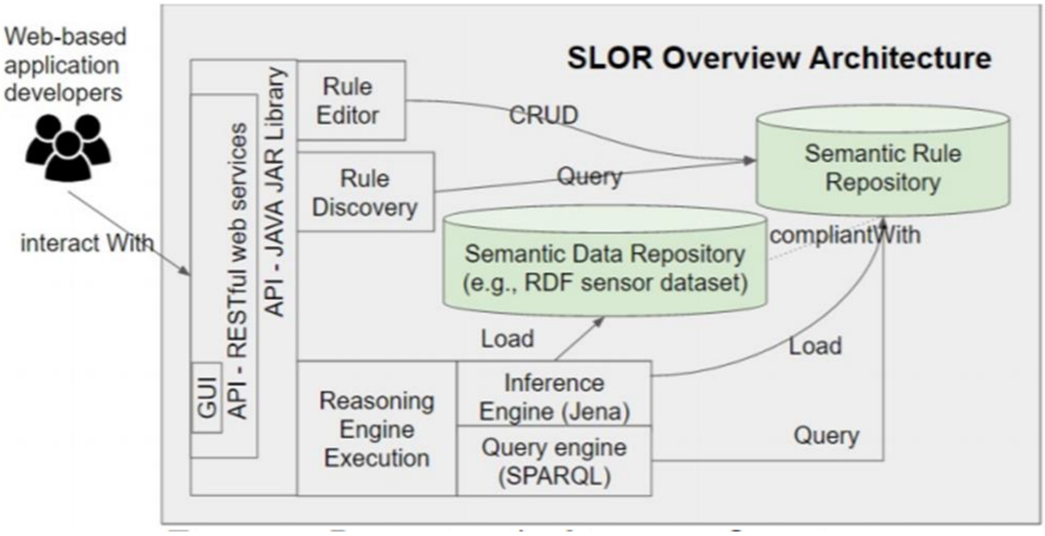

FIGURE 50 - SLOR ARCHITECTURE

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

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.

OVERVIEW

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

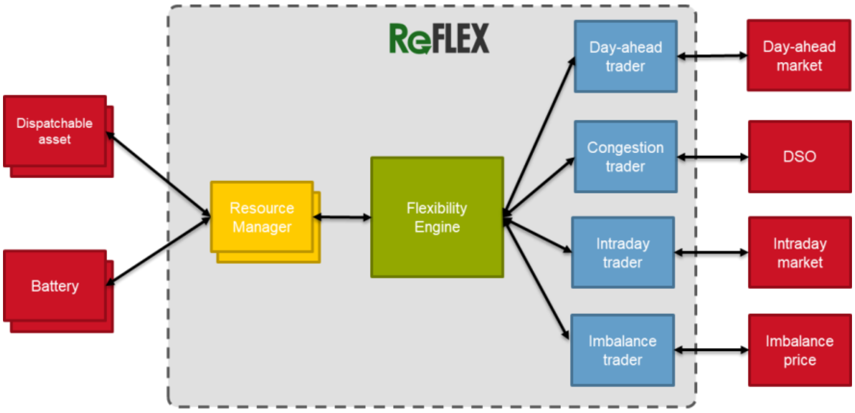

FIGURE 51 - REFLEX ARCHITECTURE

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)

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.

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>

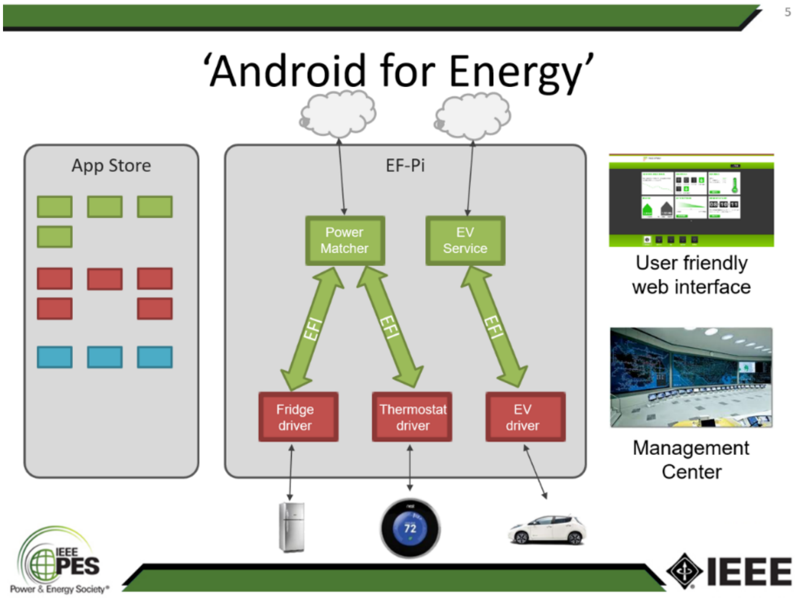

FIGURE 52 - DEF-PI ARCHITECTURE

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

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.

OVERVIEW

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

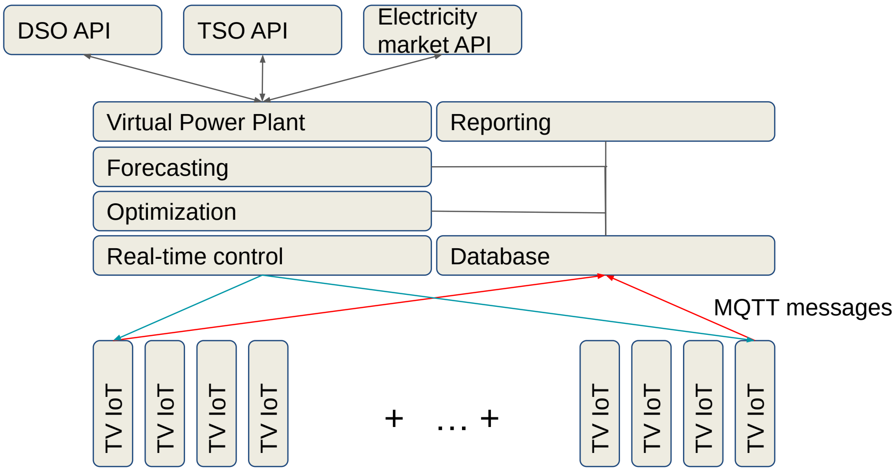

FIGURE 53 - THERMOVAULT ARCHITECTURE

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

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.

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>

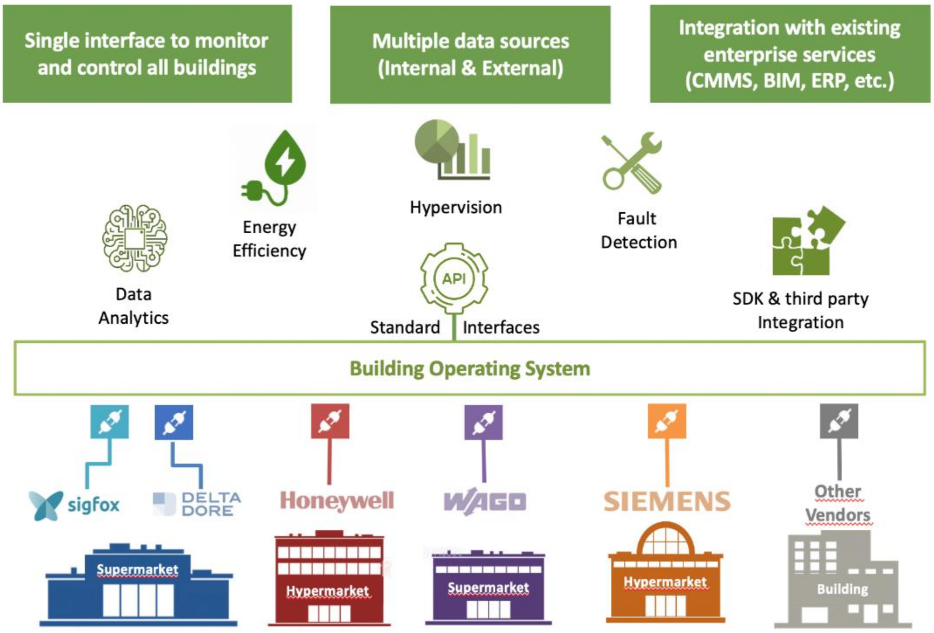
Single interface to monitor and control all buildings
Multiple data sources (Internal & External)
Integration with existing enterprise services (CMMS, BIM, ERP, etc.)
Energy Efficiency
Hypervision
Fault Detection
Data Analytics
API
Standard Interfaces
SDK & third party Integration
Building Operating System
sigfox
DELTA DORE
Honeywell
WAGO
SIEMENS
Other Vendors
Supermarket
Hypermarket
Supermarket
Hypermarket
Building

FIGURE 54 - SENSINOV ARCHITECTURE

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

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.

OVERVIEW

Platform name:
EcoStruxure Building Operation
Partner:
Schneider Electric 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>

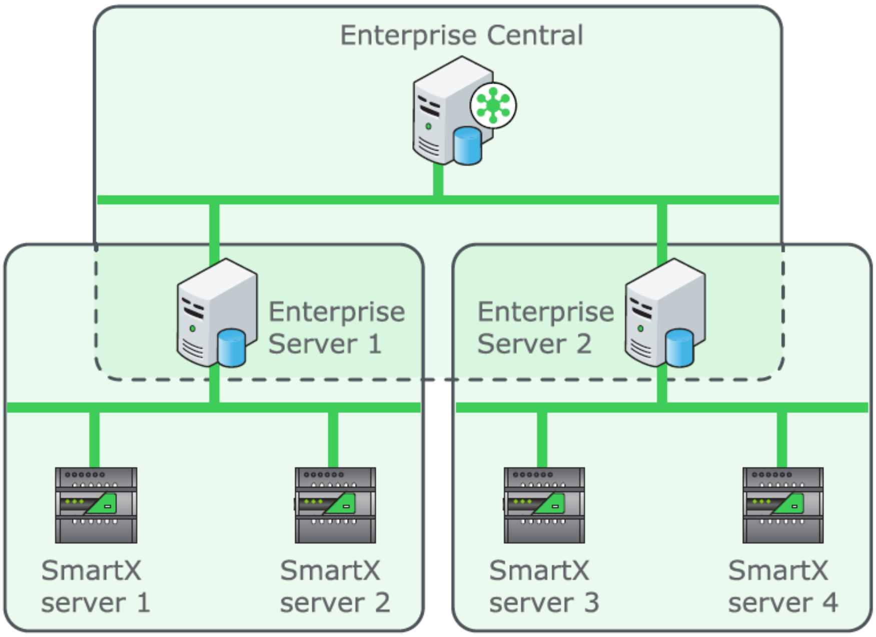

FIGURE 55 - ECOSTRUXURE BUILDING OPERATION ARCHITECTURE

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

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.

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>

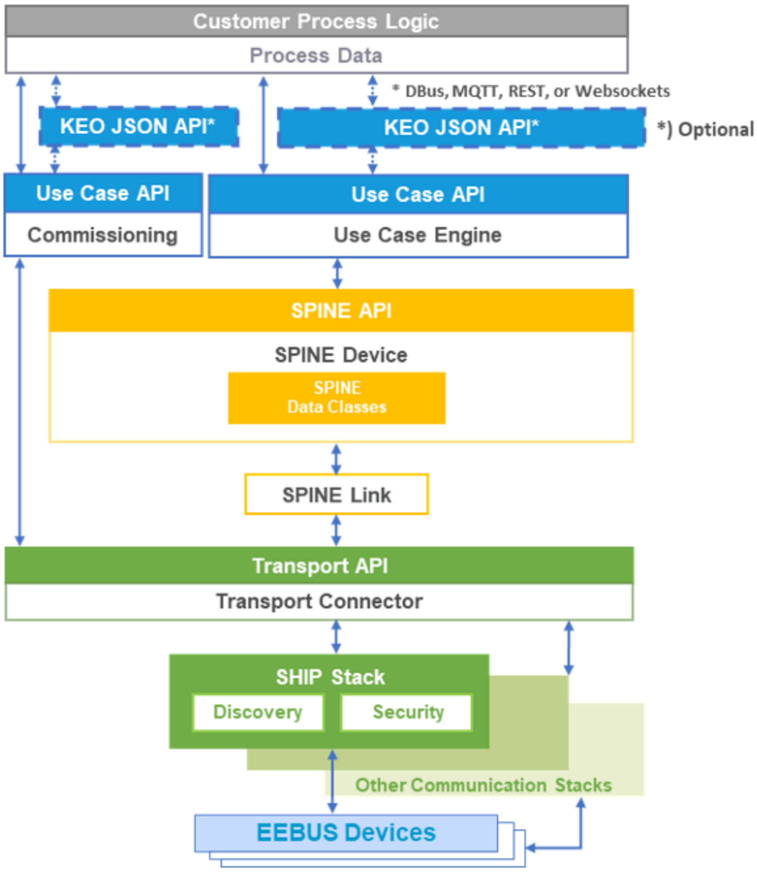

FIGURE 56 - KONECT ARCHITECTURE

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

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).

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 >

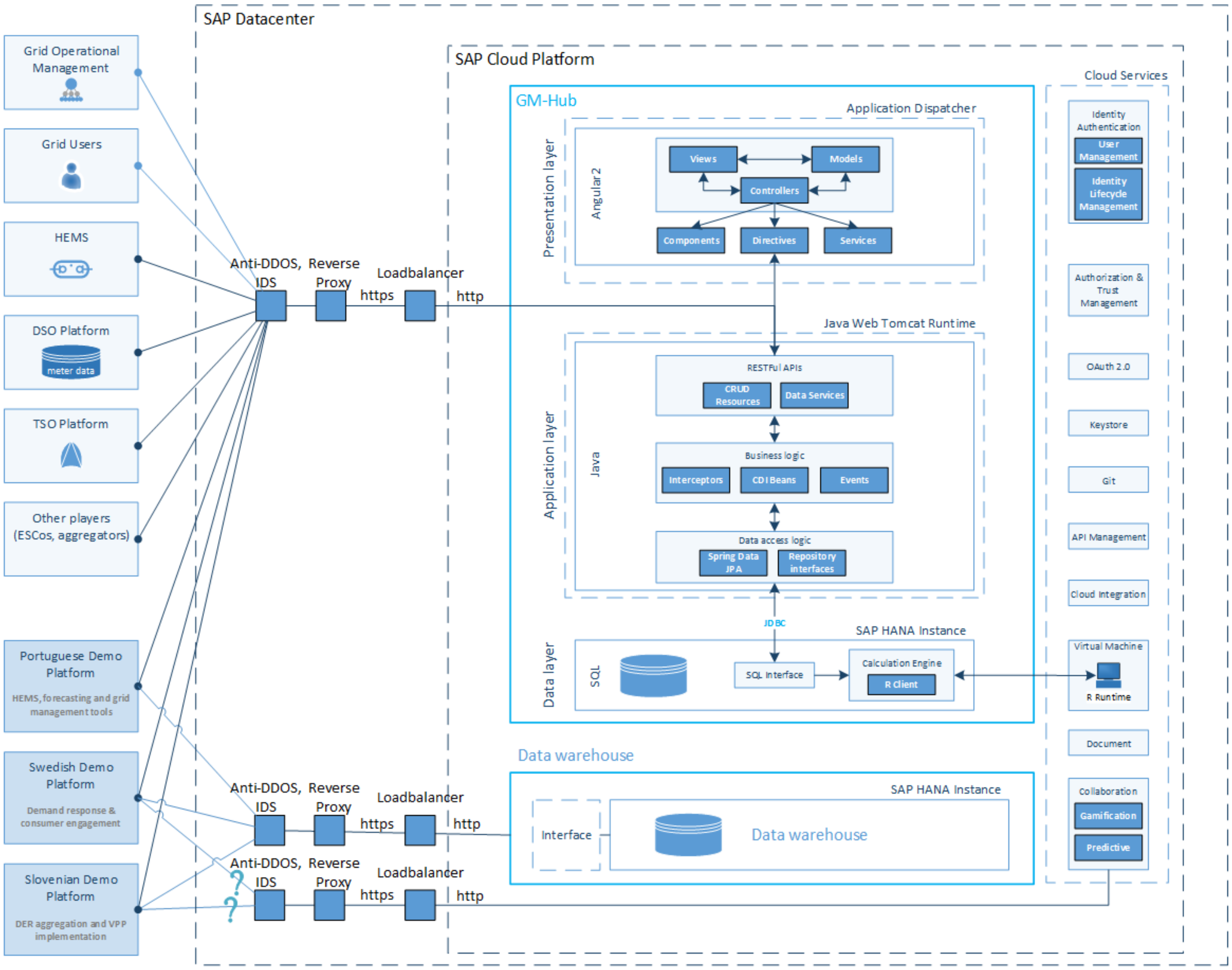

FIGURE 57 - GRID AND MARKET HUB ARCHITECTURE

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

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.

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 >

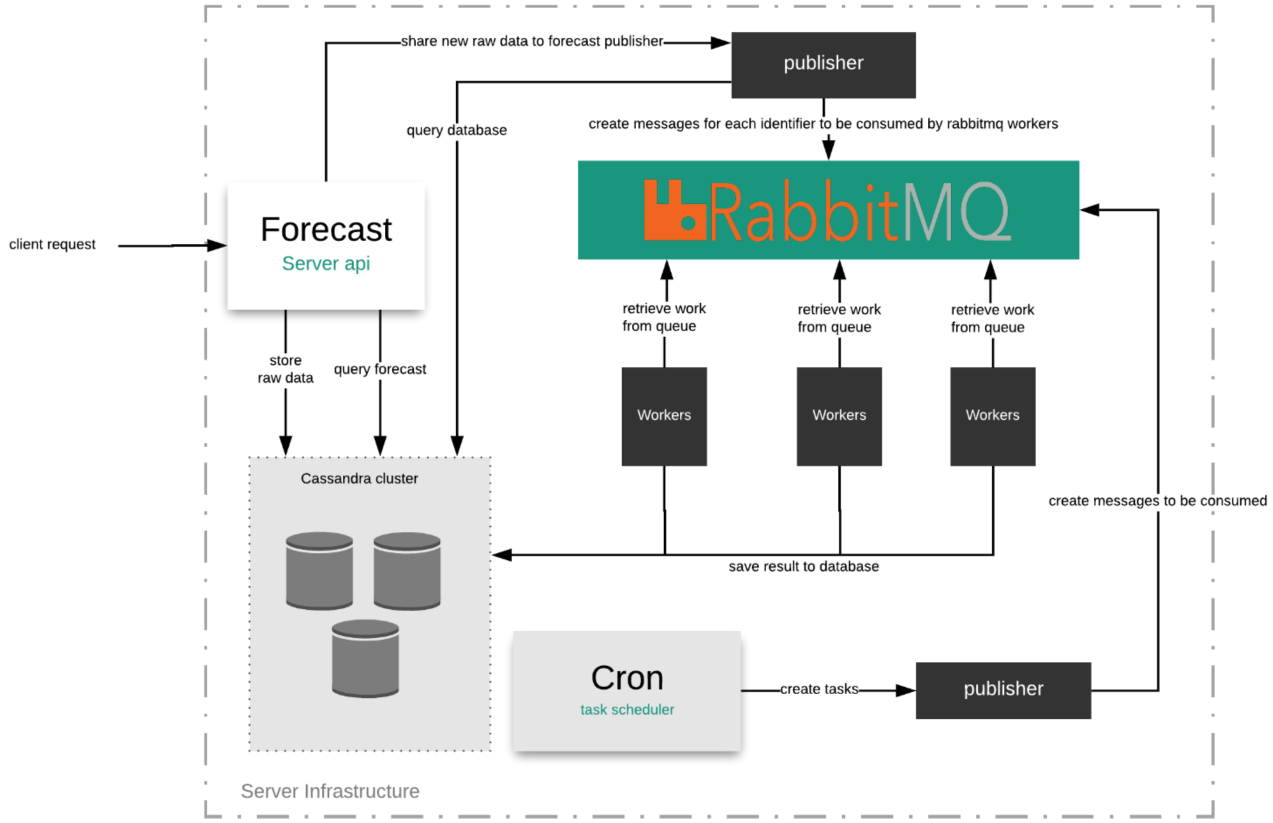

FIGURE 58 - COGNITIVE LOAD ARCHITECTURE

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

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.

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>

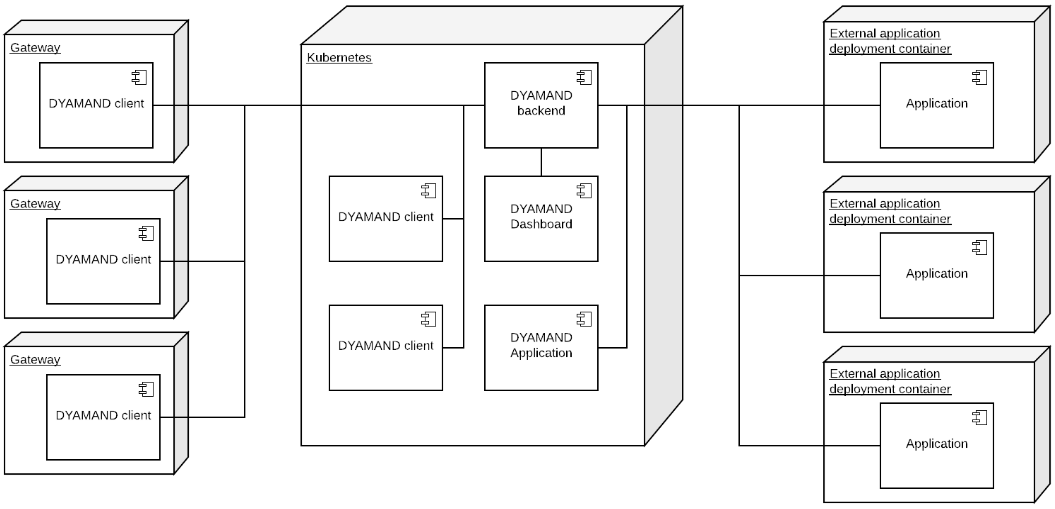

FIGURE 59 - DYAMAND ARCHITECTURE

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

EKCO 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.

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>

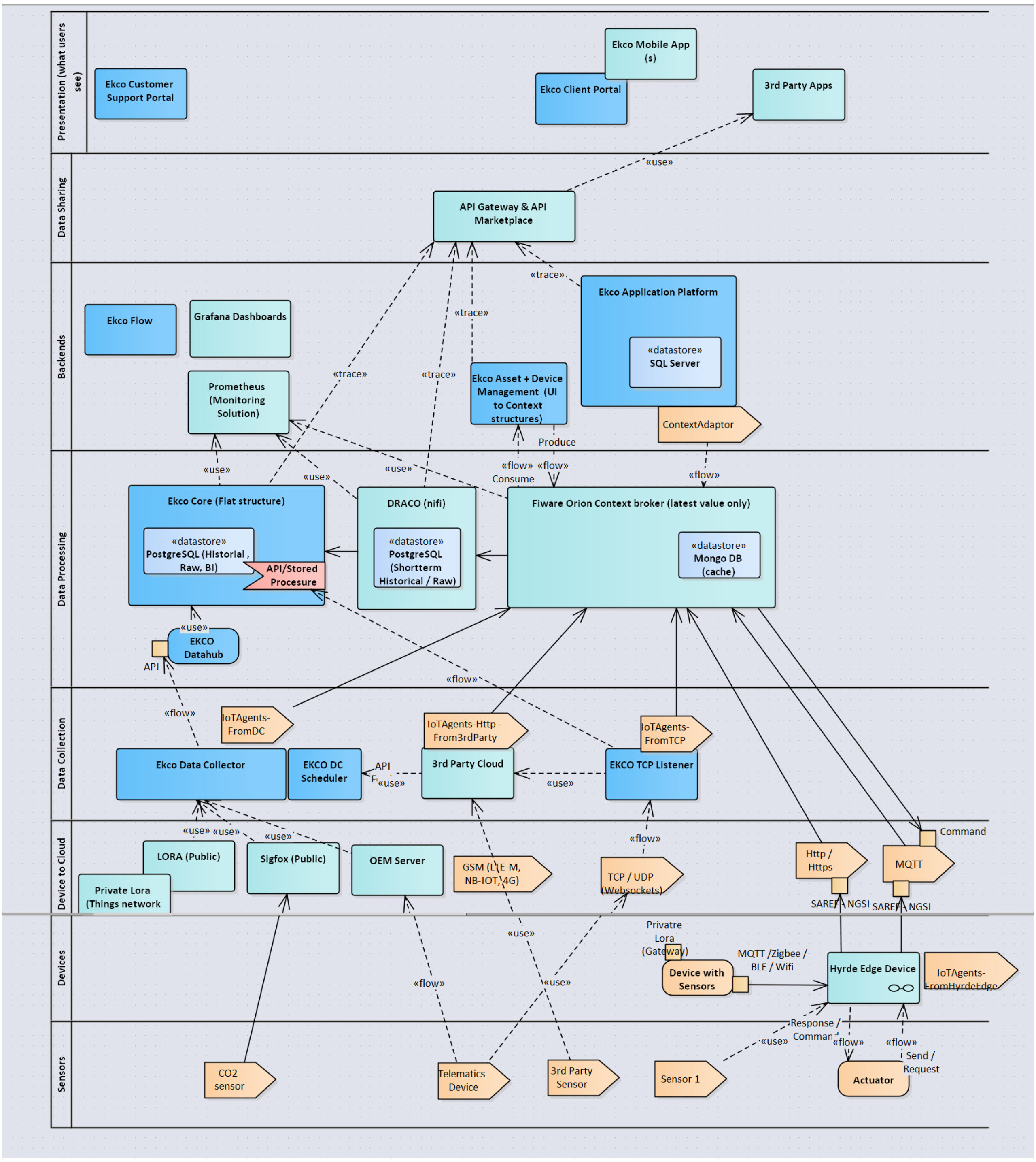

FIGURE 60 - EKCO PLATFORM ARCHITECTURE

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

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.

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>

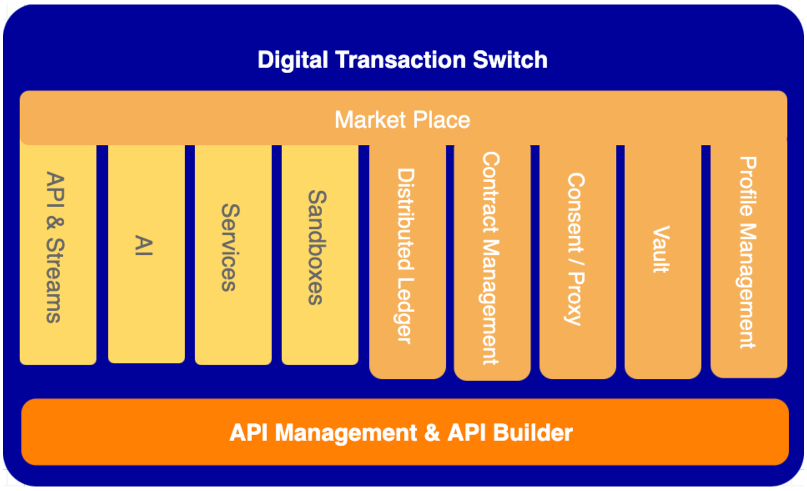

FIGURE 61 - EKCO PLATFORM

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

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.

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>

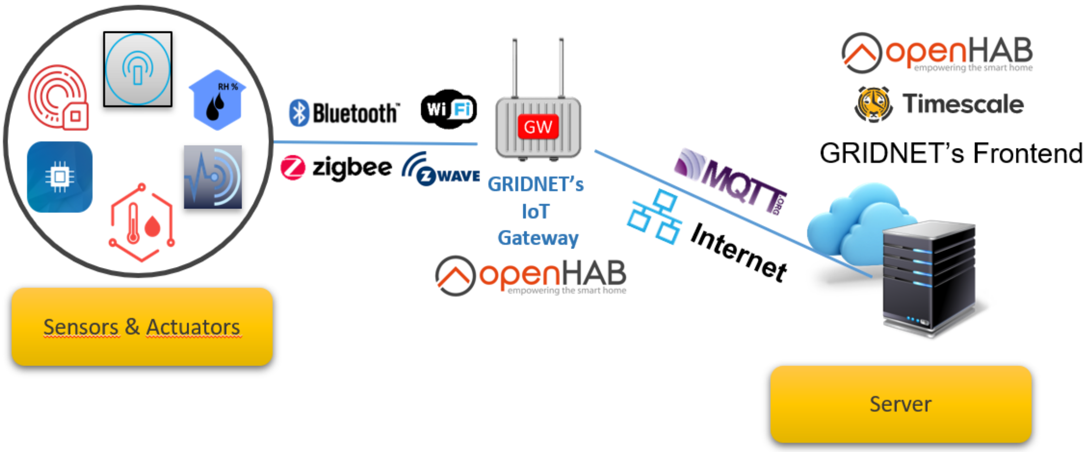

FIGURE 62 - HOMEGRID ARCHITECTURE

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

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.

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>

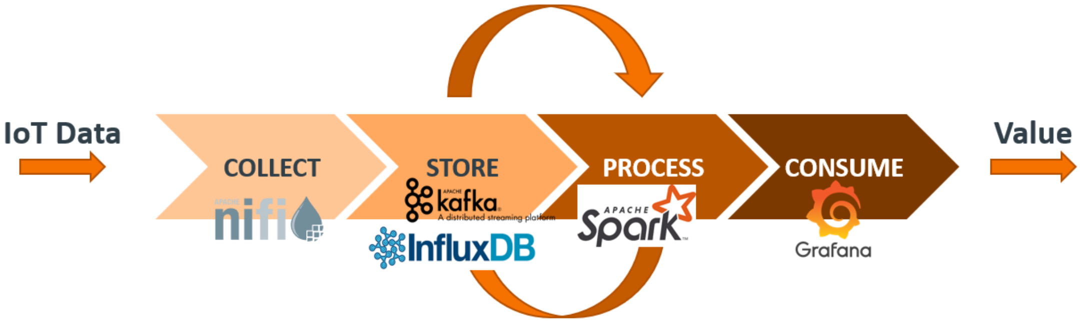

FIGURE 63 - GFI SEMANTIC IOT PLATFORM ARCHITECTURE

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

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.

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>

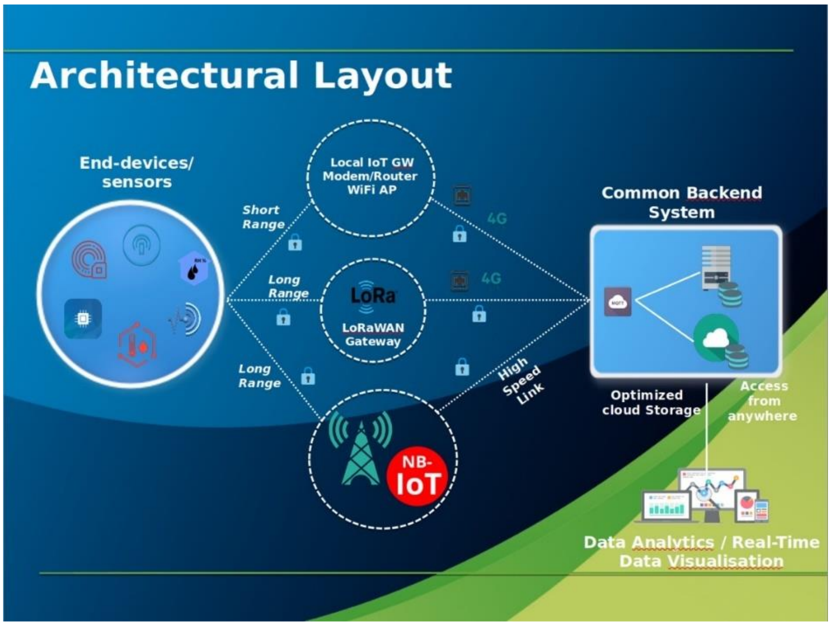

FIGURE 64 - LEONAR&DO ARCHITECTURE

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

OPENMOTICS

The platform is mainly used in 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.

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>

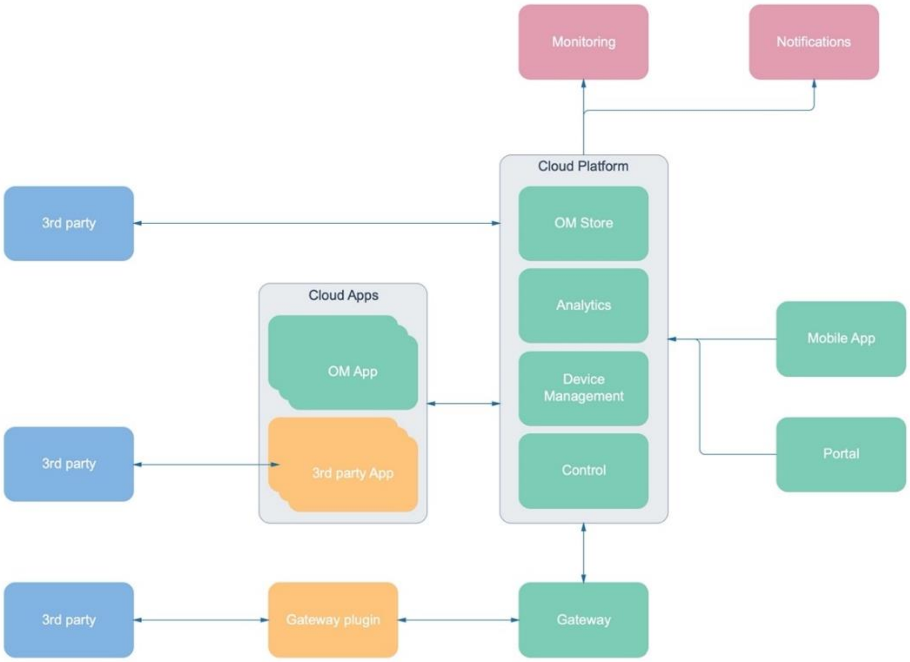

FIGURE 65 - OPENMOTICS CLOUD PLATFORM ARCHITECTURE

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

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.

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>

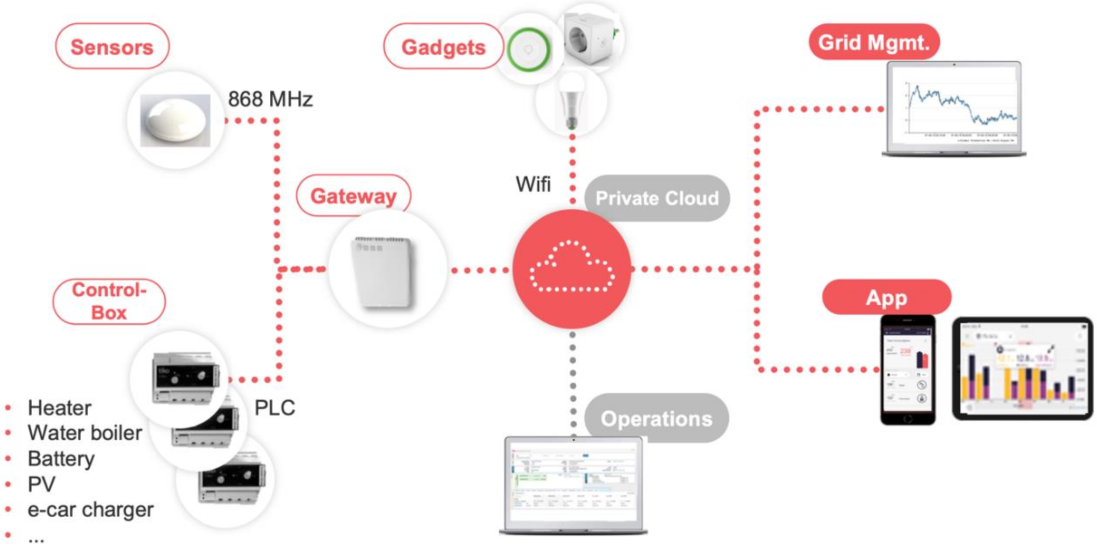

FIGURE 66 - TIKO ARCHITECTURE

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

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.

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>

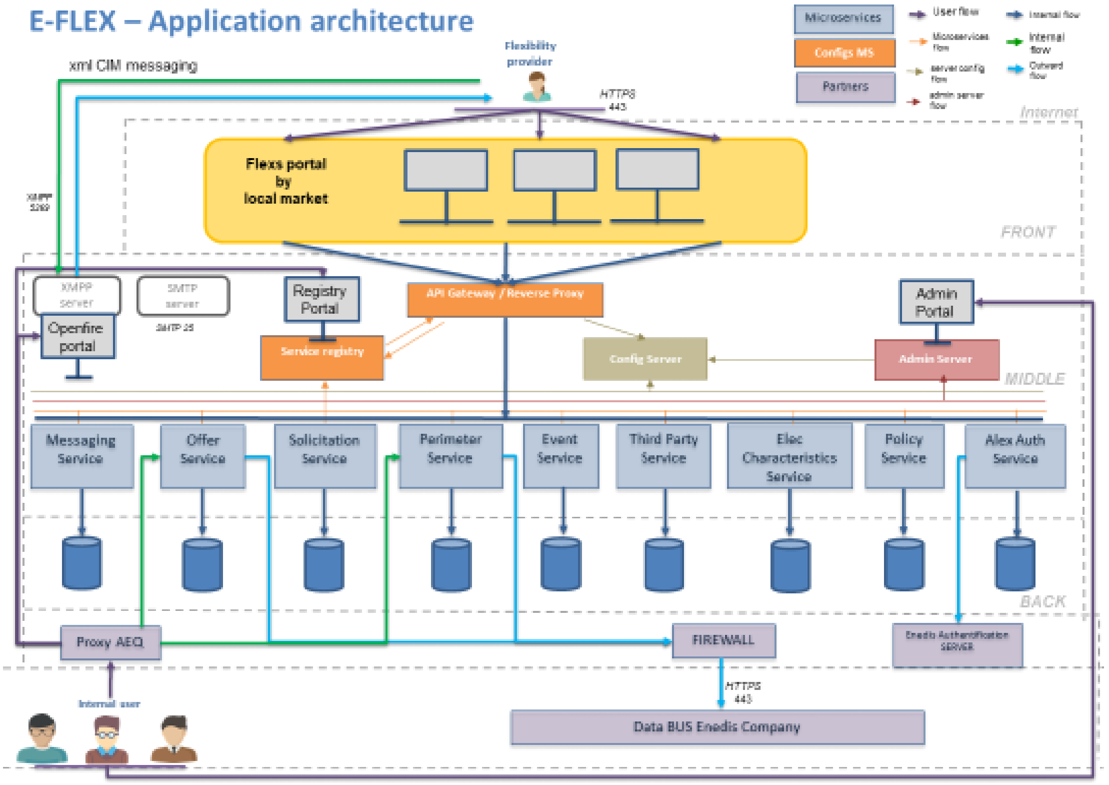

FIGURE 67 - E-FLEX ARCHITECTURE

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.

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.

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>

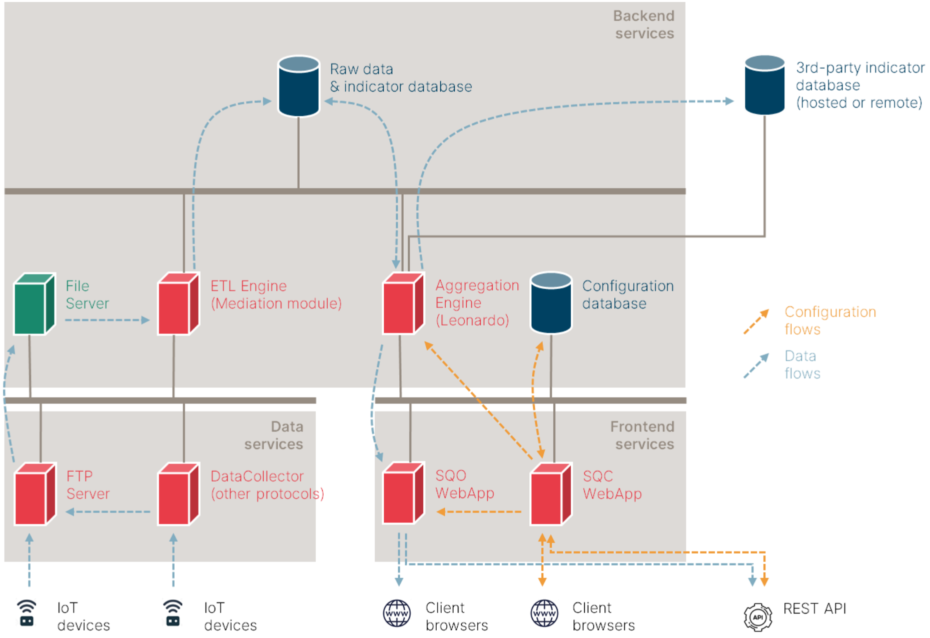

FIGURE 68 - SYNAPTIQ POWER ARCHITECTURE

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

ANNEX 2 - PILOT’S INTEROPERABILITY REQUIREMENTS AND IMPLEMENTATION STRATEGY

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.

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;

The details introduced here were collected during **months 7 to 10 of the project (April to July 2020)**. 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 were known for most pilots at this stage, our goal was to kickstart critical discussions that will continue to be carried out during the period leading to pilot implementation.

FRANCE

Pilot title	**French Pilot**
Sub-Pilot leader	**Yncréa**
Participating partners	**ENEDIS, ENGIE, GFI/Inetum (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).

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.

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.	

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 neighbourhoods.	
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 neighbourhood 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 neighbourhood 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 neighbourhoods (hydrogen cogeneration, smart windows, DC grid, V2G, interaction with neighbourhood battery that is installed on-site). The emphasis will be on the holistic approach, identified as a need for future neighbourhoods.	
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.	

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), 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.

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. 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. 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:** using 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).

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 neighbourhood 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 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 behaviour 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.

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 neighbourhood 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 Village Lab, managed by EMS:

- Charging infrastructure
- Smart houses
- Neighbourhood 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, neighbourhood).

OVERVIEW SUB-PILOT GENK

Sub-Pilot title	**ThermoVault apartments**
Sub-Pilot leader	**ThermoVault**
Participating partners	**ThermoVault**
Location	**Genk, Belgium**
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).

GREECE

Pilot title	**Greek Pilot**
Pilot leader	**GRIDNET**
Participating partners	**GRIDNET, WINGS, COSMOTE, AUEB, GFI/Inetum (BE), 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. To achieve the 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, 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, 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 analysing 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.

PORTUGAL

Pilot title	**Smart grid infrastructure as an enabler of new business demand to integrate DSF in e-markets**
Pilot leader	**E-Redes**
Participating partners	**E-Redes, 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 Interface**
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 emerges 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 describes 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 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;

GERMANY

The German pilot has two sub-pilots:

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

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	**Wirelane, Stromnetze Hamburg**

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 them later, 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.

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.

NETHERLANDS

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 data Marketplace/catalog, ReFlex**
Participating digital platforms not part of the catalogue	**Energy Monitoring Platform (VUB), Samsung SmartThings, Fiware context broker**

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 analysed (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.

ITALY

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	**Whirlpool, RSE data platform**

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.

CROSS-PILOT DEMO FOR ANCILLARY SERVICES

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 soon. 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 using 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).

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 69 and Figure 70 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 69 and Figure 70:

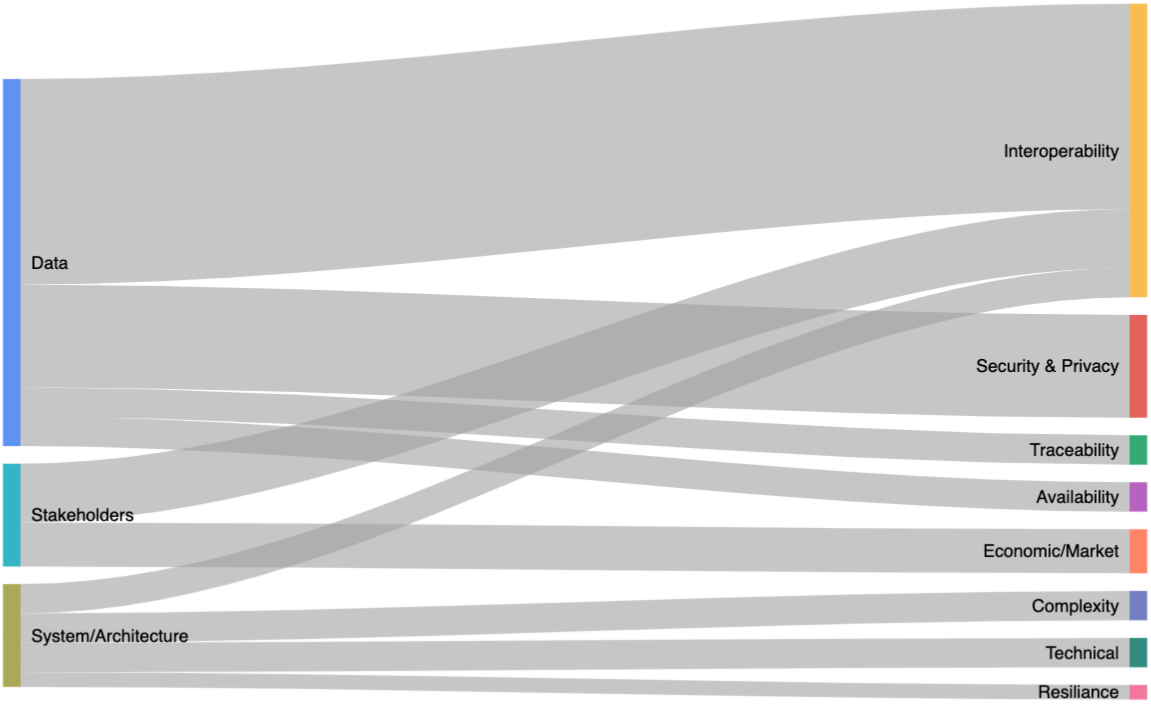

FIGURE 69 - MAIN CHALLENGES ARISING FROM CROSS-PLATFORM INTEROPERABILITY SCENARIOS

- **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.

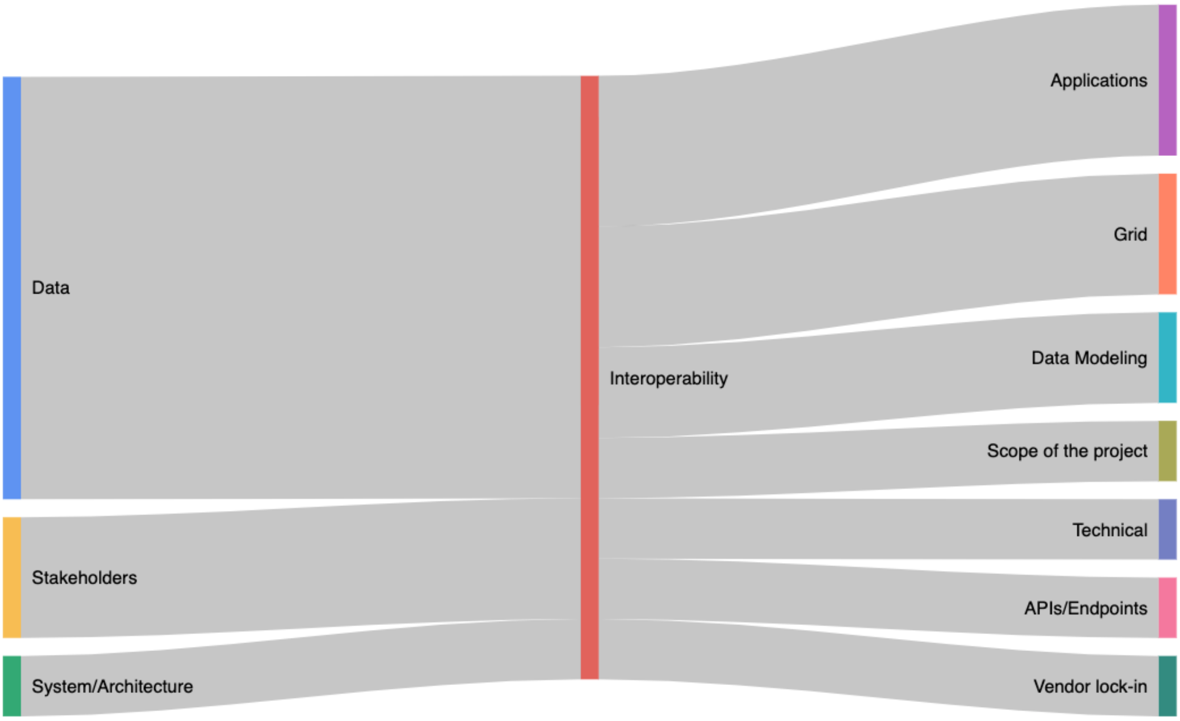

FIGURE 70 - FOCUS ON MAIN INTEROPERABILITY CHALLENGES

In terms of **opportunities**, the most cited elements are shown in Figure 71 and Figure 72, they cover the following topics:

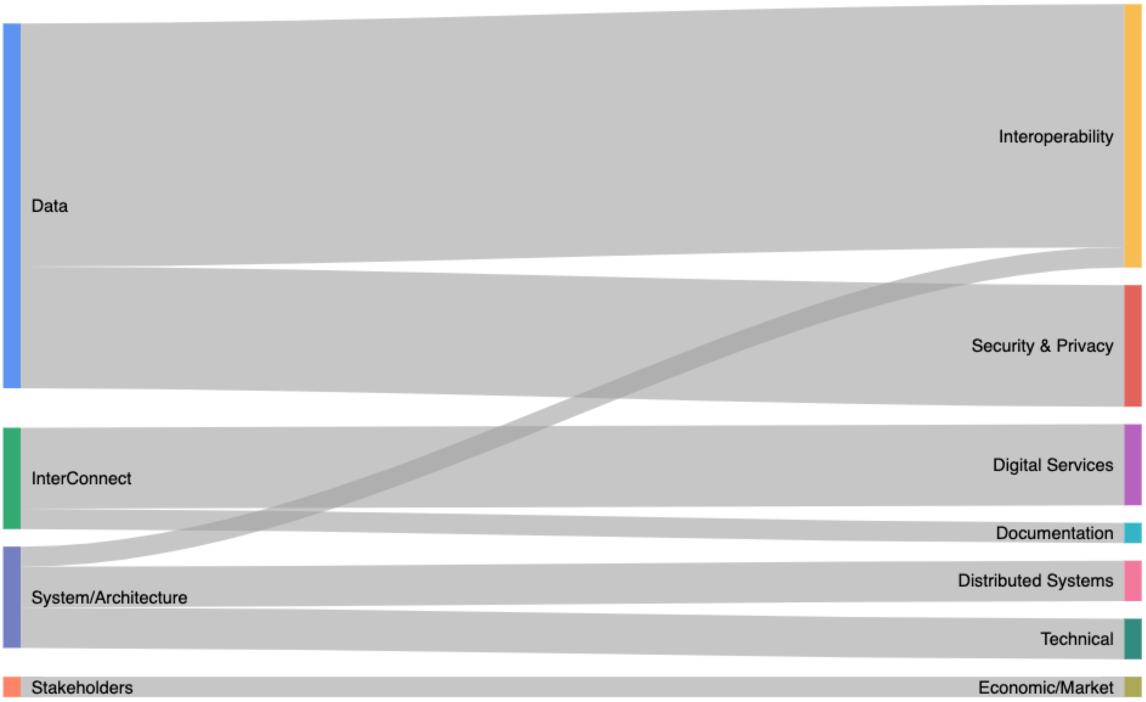

FIGURE 71 - MAIN OPPORTUNITIES ARISING FROM CROSS-PLATFORM INTEROPERABILITY SCENARIOS

- **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 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 consider 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.

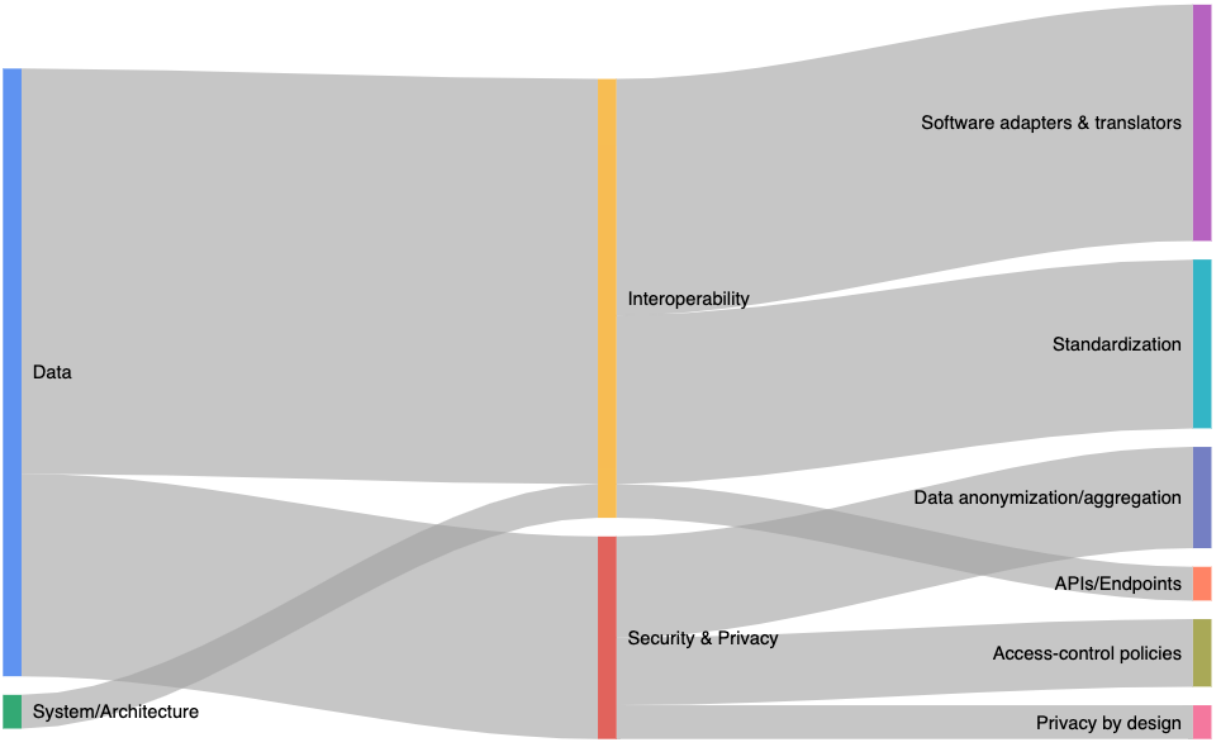

FIGURE 72 - FOCUS ON MAIN INTEROPERABILITY AND SECURITY & PRIVACY CHALLENGES

ANNEX 3 – STATE OF THE ART: COMPLEMENTARY INFORMATION

SYMBIOTE

THE SYMBIOTE REFERENCE ARCHITECTURE

The symbIoTe architecture is based on a hierarchical IoT stack, covering the following domains [3]:

- 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.

SYMBIOTE'S APPROACH TO INTEROPERABILITY

Figure 73 depicts symbIoTe's flexible and incremental approach to interoperability, introducing four compliance levels (CLs), each representing different stages of interoperability that platform providers can choose to support [3].

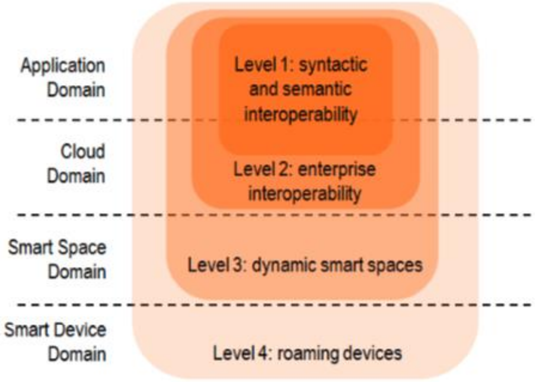
Application Domain
Cloud Domain
Smart Space Domain
Smart Device Domain
Level 1: syntactic and semantic interoperability
Level 2: enterprise interoperability
Level 3: dynamic smart spaces
Level 4: roaming devices

FIGURE 73 - SYMBIOTE COMPLIANCE LEVELS (CLS) [3]

- **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).

The interoperability patterns supported by symbIoTe are described as:

- **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.

BIG IOT

THE BIG IOT REFERENCE ARCHITECTURE

BIG IoT's architecture is based on the following building blocks:

- **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 [1]. 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.

BIG IOT’S APPROACH TO INTEROPERABILITY

As shown in Figure 74, 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*[22], that can be extended through domain-dependent or independent models. The data is then mapped to the BIG IoT Application model vocabulary.

[22] 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.

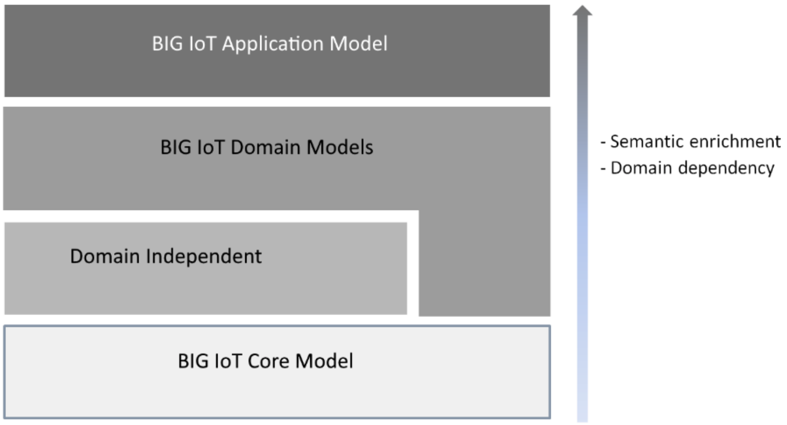

FIGURE 74 - BIG IOT'S INFORMATION MODEL (LAYERED VIEW) [1]

Data is stored in a triple store, following an RDF schema model. Once the data is expressed in an 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 performed via BIG IoT's Semantic Reasoner - a rule-based inference engine (based on a Jena inference subsystem[23]) that can generate new knowledge from data stored in triple stores[24].

INTER-IOT

INTER-IOT REFERENCE ARCHITECTURE

INTER-IoT's layered architecture introduces the following 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.

INTER-IOT'S APPROACH TO 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

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

W3C's core ontology SOSA (Sensor, Observation, Sample and Actuator) and its extension, the Semantic Sensor Network (SSN)[25].

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 are publicly available at https://inter-iot.github.io/ontology/.

Figure 75 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 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.

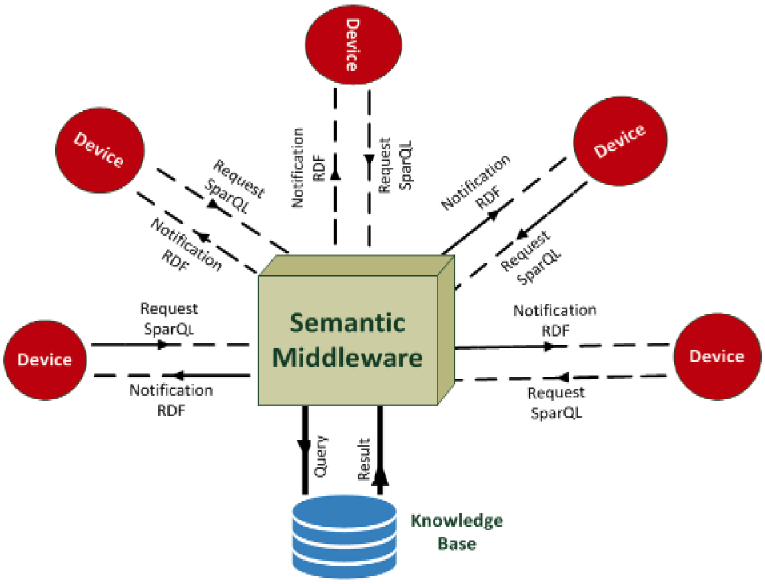

FIGURE 75 - INTER-IOT'S SEMANTIC MIDDLEWARE [5]

SINCRONICITY

SYNCHRONICITY'S REFERENCE ARCHITECTURE

The project's reference architecture is built around a set of logical [6], 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. Data security and quality are guaranteed by integrating aspects such as data anonymization and categorizing (i.e., public/open, or private data).

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

- 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 SynchroniCity. 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.

SYNCHRONICITY'S APPROACH TO INTEROPERABILITY

SynchroniCity's data model builds on OASC's reference information meta-model (OMA NGSI meta-model, shown in Figure 76), commonly used on smart city projects [7].

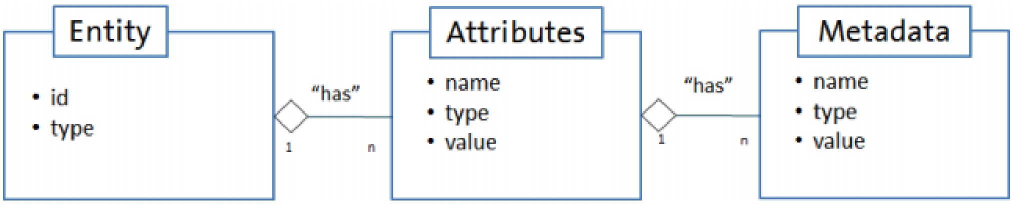

FIGURE 76 - OMA NGSI META-MODEL [7]

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].

VICINITY

VICINITY'S REFERENCE ARCHITECTURE

VICINITY's architecture is based on a peer-to-peer (P2P) network of nodes, which allows 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).

VICINITY'S APPROACH TO INTEROPERABILITY

VICINITY's semantic interoperability is realised thanks to the project's modular core information model[26], which can be extended through different domain-specific and cross-domain modules, based on use case and partners requirements.

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.

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.

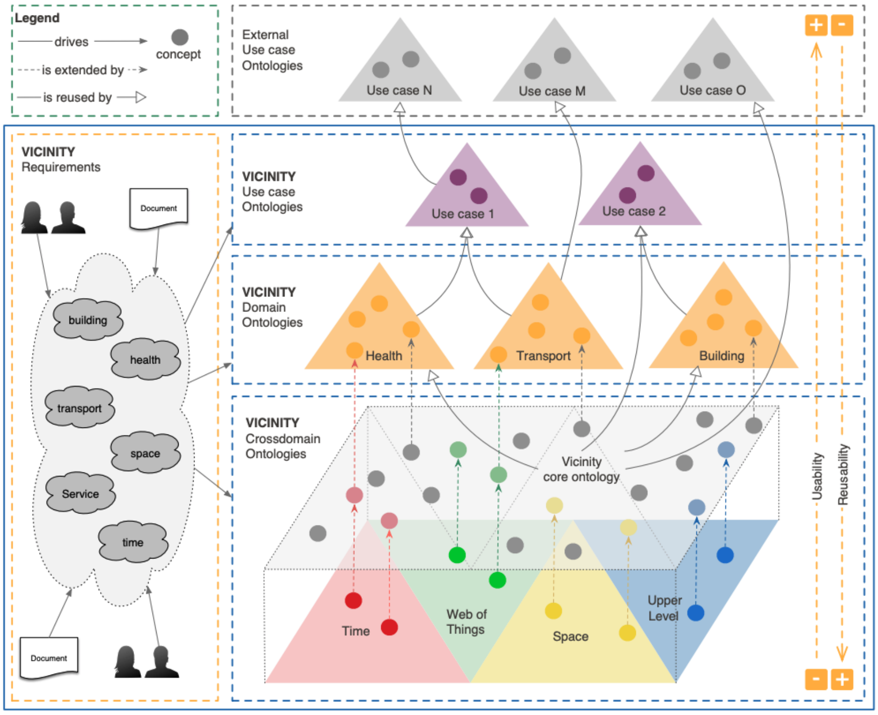

FIGURE 77 - VICINITY'S ONTOLOGY DESIGN [8]

FIESTA-IOT

FIESTA-IOT REFERENCE ARCHITECTURE

The project's functional architecture introduces the following key components:

[26] http://iot.linkeddata.es/def/core/index-en.html

- 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 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).

FIESTA-IOT'S APPROACH TO INTEROPERABILITY

FIESTA-IoT's approach to semantic interoperability is built around the FIESTA-IoT Ontology. As shown in Figure 78 the project's ontology merges useful concepts from existing ontologies into one [9].

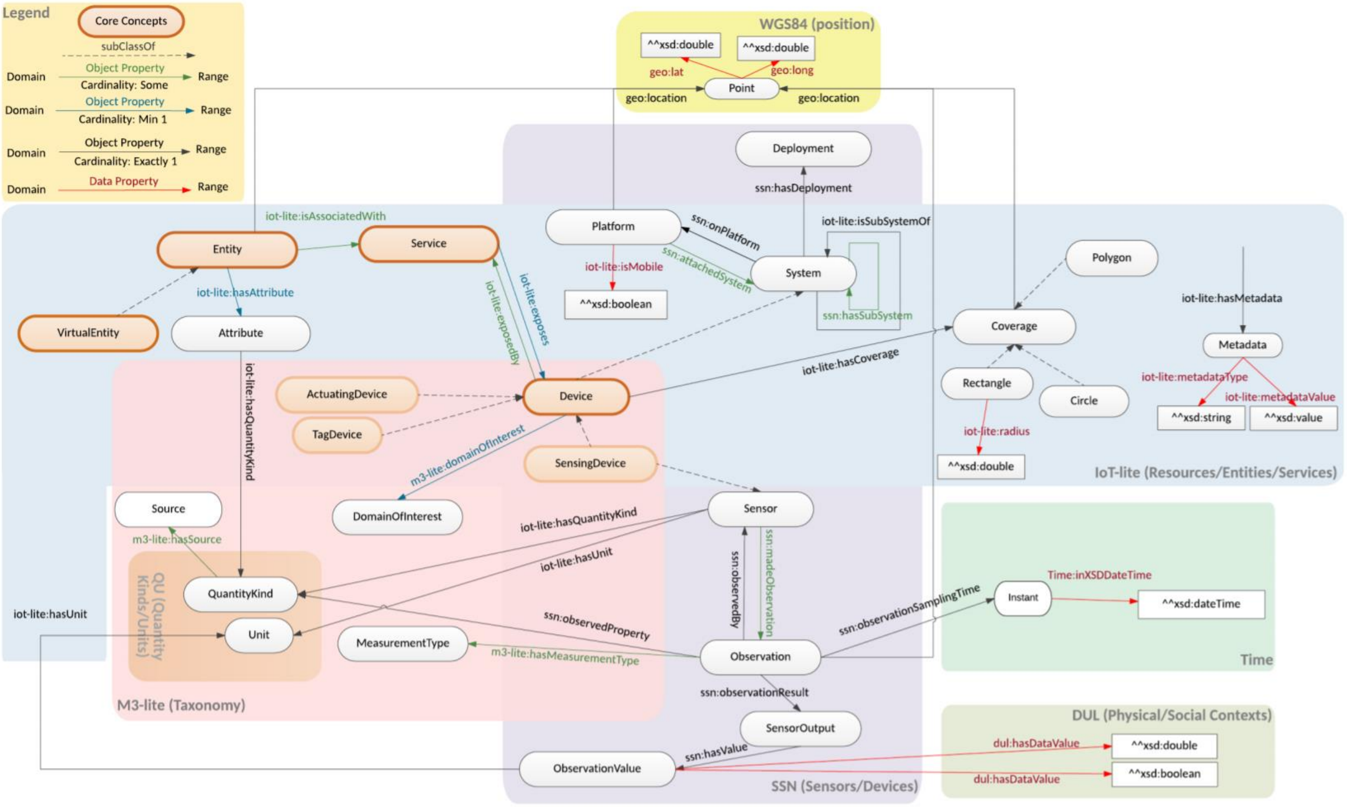

FIGURE 78 - THE FIESTA-IOT ONTOLOGY [9]

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.

AGILE IOT

AGILE IOT'S REFERENCE ARCHITECTURE

The software stack can be divided into two main bundles: 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,
    - 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 recommendation to the project's end-users.

AGILE IOT'S APPROACH TO INTEROPERABILITY

This project does not define an approach for semantic interoperability.

BIOTOPE

BIOTOPE'S REFERENCE ARCHITECTURE

bIoTope's architectural framework, which can be described as a highly flexible and dynamic ecosystem, built around the Micro-Services Architecture (MSA) paradigm [10]. 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[27]. 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 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 then 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[28] 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 custom 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).

[27] https://www.opengroup.org/?gclid=CjwKCAjwqML6BRAHEiwAdquMncLVtncwP5flrhl9RlDdZjnJ4iAU9GG3FhAVjKFy76CGJ7ob9ETqFBoCeV4QAvD_BwE

[28] **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.

BIOTOPE’S APPROACH TO INTEROPERABILITY

bIoTope’s semantic interoperability approach is presented in [10]. 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 can be used depending on specific requirements to cover domain-independent or domain-specific descriptions.