



**interoperable solutions  
connecting smart homes,  
buildings and grids**

## **WP5 – Digital Platforms and Marketplace**

### **D5.3**

**Security, cybersecurity and privacy protection  
action plan and results**



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

## DOCUMENT INFORMATION

DOCUMENT	D5.3 – Security, cybersecurity and privacy protection action plan and results
TYPE	Report
DISTRIBUTION LEVEL	Public
DUE DELIVERY DATE	31/03/2021 (submitted)
DATE OF DELIVERY	08/04/2021 (resubmitted (30/09/2021))
VERSION	v3.0
DELIVERABLE RESPONSIBLE	Trialog
AUTHOR (S)	Trialog: Antonio Kung, Estíbaliz Arzoz Fernández, Amélie Gyrard, Milenko Tosic (VLF) Fábio Coelho, David Emanuel Rua (INESC TEC)
OFFICIAL REVIEWER/s	Milenko Tosic (VLF) Fábio Coelho (INESC TEC) David Rua (INESC TEC) Gjalt Loots (TNO) Laura Daniele (TNO)

## DOCUMENT HISTORY

VERSION	AUTHORS	DATE	CONTENT AND CHANGES
0.1	Estíbaliz Arzoz Fernández	16/02/2021	Table of Contents
0.2	Antonio Kung	08/03/2021	Section 2
0.3	Estíbaliz Arzoz Fernández	09/03/2021	Update Sections 3 to 10
0.4	Estíbaliz Arzoz Fernández	11/03/2021	Update Sections 3 to 11
0.5	Estíbaliz Arzoz Fernández	16/03/2021	Update Sections 3 to 10
0.6	Antonio Kung	18/03/2021	Update of section 2 further to internal project review
0.7	Fábio Coelho, Milenko Tosic, Estíbaliz Arzoz, Antonio Kung	29/03/2021	Internal check, and update to include review recommendations
1.0	Fábio Coelho, Milenko Tosic, Estíbaliz Arzoz, Antonio Kung	31/03/2021	Final version submitted to the European Commission
2.0	David Rua, Paulo Monteiro	01/04/2021	Revision and document formatting
2.1	David Rua, Paulo Monteiro	02/04/2021	Revision and document formatting
2.2	David Rua, Paulo Monteiro	03/04/2021	Revision and document formatting
2.3	David Rua, Paulo Monteiro	04/04/2021	Final version submitted to the European Commission
2.4	Antonio Kung, Estíbaliz Arzoz, Milenko Tosic, Fábio Coelho	23/09/2021	Refactoring of the document to account for European Commission comments.
3.0	Milenko Tosic, , Antonio Kung, Estíbaliz Arzoz	30/09/2021	Final version submitted to the European Commission

## ACKNOWLEDGEMENTS

NAME	PARTNER
Arnor Von Leemputen	Th!nk-E
Chaim De Mulder	Openmotics
Ectors Dominic	VITO
Thierry Coosemans	VUB
Mojtaba Eliassi	3E
Esteban Municio	University Antwerp - Imec
Pol Olivella	ThermoVault
Anais Galligani, Stéphane Vera	Yncrea
Stefano Fava	PlanetIdea
Robert Healey	Formiti (DPO in charge of the Italian pilot)
Ullrich Bartsch	EEBUS
Thomas Fishedick	Keo Connectivity
Wouter Beelen, Niels Ten Brick	Volkerwessels
Andraz Andolsek	CyberGrid
Donatos Stravropoulos	Gridnet
João Falcão	E-Redes

## 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.*

## ABSTRACT

This deliverable covers the actionable Security and Privacy protection Plans (SPP) of the pilots of the H2020 InterConnect project, an IoT large-scale project focusing on smart energy, smart buildings, and smart homes. The work carried out in this deliverable consisted of the following activities and results:

- Specifying SPP templates for streamlining the process of collecting information from the pilots and the interoperability framework development team. This work is based on the SPOCS (Security and privacy POLicies Compliance Solution) approach documented in [1].
- **Stage 1 SPP preparation** - Defining a first version of the actionable plans for all the pilots focusing on the definition of the context in which pilot ecosystems will be established. Templates were provided to support a generic analysis of the InterConnect interoperability framework security and privacy/data protection capabilities. At this stage SPP of the interoperability framework was drafted.
- **Stage 2 SPP preparation** - Defining a second version of the actionable plans focusing on the identification of threats, risks, and measures for their treatments. A final characterisation of the InterConnect interoperability framework security and privacy protection capabilities was prepared. Finally, individual pilot security and privacy risk analysis was carried out and lists of security and privacy measures were identified.

## EXECUTIVE SUMMARY

### Background

The H2020 InterConnect project aims to provide an efficient energy management through an ecosystem where demand flexibility can be integrated with comfort and convenience for end-users. The core technical challenge being to ensure semantic interoperability between services, digital platforms, devices, and applications in cross domain scenarios (IoT and energy). To that end, InterConnect implements, deploys and assesses the application of an interoperability framework (IF – designed in WP2/WP5 and implemented in WP5 as documented in D2.1 [2] and D5.1 [3]) that enables the semantic and syntactic interoperability required by a large set of use cases (collected and documented in WP1) on seven large-scale pilots (prepared in WP6 and implemented in WP7).

Each pilot represents an ecosystem where different actors are involved, collecting and sharing data for the services to be provided to end-users based on an initial set of use cases, which in a later stage will enable even more innovative use cases, once the interoperability framework currently established will become more mature. It is important to note that the digital platforms used by each pilot are mature platforms on high TRL already adopted in research and commercial projects. Each of those platforms comes with its set of cybersecurity and privacy protection capabilities. The interoperability framework is supplied to the digital platform owners and service providers as a set of tools to help them achieve semantic interoperability (relying on SAREF family of ontologies). Achieved semantic interoperability of participating platforms and services leads to establishment of semantically interoperable ecosystems representing the project pilots. In order to implement actionable procedures which are complementary and do not impact security and privacy protection requirements and practices of the platform operators, a Security and Privacy protection Plan (SPP) has been created for the interoperability framework. The interoperability framework SPP is then supplied to the project pilot teams as one of the inputs necessary for drafting, agreeing on and maintaining pilots' own actionable SPPs.

Besides enabling interoperability at the technical level, a critical issue is to ensure security and privacy in the complex cross domain ICT ecosystems represented by the InterConnect pilots. In each ecosystem multiple digital systems and stakeholders are involved. There are valuable references that provide guidance on creating actionable security plans<sup>1</sup> or privacy plans<sup>2</sup>, but none of them combine security with privacy, nor take into account the cross-domain ecosystem dimension. The InterConnect semantically interoperable ecosystems (project pilots) are in fact system of systems and as such introduce a new set of challenges for drafting and applying actionable SPPs. Previous projects in the European IoT Platform Initiative projects<sup>3</sup> tackled the challenge of security and privacy protection among federated and interoperable IoT platform. Similarly, the Create-IoT<sup>4</sup> provides guidelines on how to document and manage

---

<sup>1</sup> For instance, NIST Guide for security plans 2006 (<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-18r1.pdf>), or ISO/SAE 21434 Road vehicles cybersecurity engineering

<sup>2</sup> For instance, ISO/IEC 27570 Privacy guidelines for smart cities

<sup>3</sup> <https://iot-epi.eu/>

<sup>4</sup> <https://european-iot-pilots.eu/project/create-iot/>

security and data protection capabilities and measures in large scale IoT pilots involving multiple stakeholders and digital systems. InterConnect utilizes best practices from these projects in preparing templates for documenting SPPs (focusing on right information, challenges, and relationships), securing IF and properly defining privacy protection jurisdictions between the IF and pilots as well as measures to be taken (more detailed analysis of these projects is presented in D2.2 [1]).

### Contribution

The objective of the work presented in this deliverable was to define a security and privacy protection practice that can be applied by all pilots in a context where:

- Pilot is an ecosystem embarking into the development and integration of smart energy services.
- Pilot is using the InterConnect interoperability framework for establishing semantic interoperability between participating systems (digital platforms, services, and devices).
- Pilot must carry out a security and risk analysis that allows it to identify the needed risk treatments, leveraging the security and privacy enablers coming with the InterConnect interoperability framework as well as security and privacy capabilities and limitations of participating systems (digital platforms, services, and devices).
- Pilot must learn the process of negotiating the security and privacy capabilities with suppliers.

The scope of the work is the following:

- To investigate best practices and standard approaches for creating security plans (NIST, ISO/SAE and ISO/IEC families of standards), privacy plans (e.g., ISO/IEC 27570) and conducting threat and risk analysis from perspective of security (e.g., STRIDE) and privacy (e.g., LINDDUN).
- To specify a template for a pilot security and privacy protection plan (further called SPP), considering the need to carry out integration work with the supplier of the InterConnect interoperability framework, digital platform operators, service providers and device manufacturers.
- To conduct detailed security and privacy protection analysis and specification of measures and concrete techniques to be used by the interoperability framework.
- To support the updates of the SPP, as security and privacy activities are continuous, and require maturity (e.g., IEC 62443 specifies a security program rating as the combination of a security level and a maturity level).
- Stage 1 - support the pilots in the definition of the first version of their security and privacy plan focusing on capabilities of the digital systems comprising the pilots.
- Stage 2 - support the pilots in their security and privacy risk analysis, considering the security and privacy capabilities of the InterConnect interoperability framework to validate the security and privacy measures, and update their security and privacy plan making it ready for realization/pilot deployment.

A first report corresponding to stage 1 was prepared in March 2021. This updated report includes updated SPP of the interoperability framework and stage 2 SPP evolution of the project pilots focusing on risk and threat analysis and measures to be taken for their mitigation. The stage 2 report does not replace stage 1 report, as it is important, for a good SPP practice,

to keep versions in the ecosystem security and privacy documentation system, to trace decisions back and fix them when there is a security or privacy breach.

The work presented in this deliverable concludes that the results from the SPP practice can be adopted in future EC projects or industry deployments and be standardized<sup>5</sup>.

## Approach

The following approach was taken when specifying SPPs for the pilots and the interoperability framework:

- Each pilot is an ecosystem or system of systems provided by multiple independent stakeholders (digital platform operators, service providers, device manufacturers and interoperability framework provider).
- There is a single SPP per pilot, covering the entire scope of the pilot and addressing all participating systems, interoperability framework instance and relationships and agreements made by the stakeholders towards realization of the use cases.
- The interoperability framework stakeholder(s) are suppliers of enablers and services for facilitating semantic interoperability within and among pilot ecosystems. There are other semantically interoperable services (energy and non-energy) utilized by the pilots and managed by project partners/service providers.
- Stakeholders participating within the pilots negotiate and define management plans in line with the SPP template. These plans and decision are mostly on the policy level and correspond to the overall objectives of the pilots as well as exploitation plans of the participating partners.
- The pilot negotiates an operating agreement with the interoperability framework supplier. As a result, the supplier provides information on the interoperability framework security and privacy capability. The agreement follows the project grant agreement and consists of (this approach is also valid for integrators outside of the project consortium):
  - Business agreement in line with the interoperability framework exploitation strategy. This strategy is still in development.
  - Service agreement including different interoperability framework deployment and integration options each with its set of cybersecurity, access control and data protection capabilities and requirements. Privacy protection jurisdictions are clearly defined for different framework deployment options. This guides pilot stakeholders towards proper privacy protection decisions when proceeding to send potentially sensitive data to other interoperable stakeholders and through the instantiated semantically interoperable layer.

During stage 1 preparation of the SPPs, the following approach was applied:

- The recommendations of ISO/IEC 27570 (privacy guidelines for smart cities) for the use of a privacy plan were followed, covering five parts:
  - a governance management plan,
  - a data management plan,

---

<sup>5</sup> Several presentations have been made, including during the IEEE 7<sup>th</sup> world forum on internet of things special session on EC projects (<https://wfiot2021.iot.ieee.org/program/plenary-program/>), or in the AIOTI standardisation WG, with a plan to discuss with ISO/IEC JTC1/SC27 or SC41 to possibility to create a standard.



- a risk management plan,
  - an engineering management plan, and
  - a citizen management plan.
- A template was used to characterise the generic security and privacy capability of the InterConnect interoperability framework, consisting of the following:
  - actors, use cases and architecture entities,
  - a description of the security and privacy capabilities of the interoperability framework components.
- Another template was provided to carry out a generic security and risk analysis of the interoperability framework covering:
  - threats, breaches, and their relation,
  - impacts of the threats and breaches,
  - measures to manage the threats and mitigate the risks/impacts,
  - Guidance was provided for threat analysis based on STRIDE and LINDDUN, risk maps, and lists of security and privacy controls based on ISO/IEC 27001 and ISO/IEC 27701.

During stage 2 the following approach was applied:

- A final characterisation of the security and privacy capability of the InterConnect interoperability framework, as well as those of the project pilots, were conducted covering the following categories of actionable measures:
  - information security policies (information security organization, incident management and aspects of business continuity management),
  - asset management, access control, and cryptography applications,
  - operation security and communication security,
  - system acquisition, development, and maintenance with suppliers' relationships.
- Security and risk analysis were carried out for each project pilot leveraging security and data protection capabilities of the interoperability framework as well as inherent capabilities of the participating digital platforms.

## Results

Stage 1 version of the deliverable focused on the creation of the first draft of SPPs for project pilots and the InterConnect interoperability framework. Detailed definition of the security and privacy protection features of the interoperability framework are documented. Different deployment options and access configuration options of interoperability framework are documented. This was to be used as a basis for each project pilot when deriving detailed management plans of their SPPs. Stage 1 document included the first iteration of SPPs from all project pilots. Due to pilots' development and negotiation stage not being finished, certain pilots have yet to work on precisising measures and procedures behind their SPPs.

Stage 2 version of the deliverable report focused on finalising the security and privacy actionable measures to be implemented for each pilot. Risk and threat management plan for each pilot is defined. Threat identification is conducted and corresponding mitigation/treatment is identified. A starting point for each pilot is SPP and risks/threats/measures of the interoperability framework as well as risks and measures identified for each digital system comprising the pilot. On top of that, new risks, threats and corresponding measures are identified resulting from the integration challenges raising from the project use cases.



Security capabilities of IF include: protected tunnels for unified communication interface between interoperable services, configurable access control and recipient selecting as part of the semantic interoperability layer, authentication and authorization that can be applied on each data exchange request. The IF is not processing or storing data exchanged between interoperable services, it only relays the data. Only metadata, describing capabilities and interactions of interoperable services are stored by IF, and integrators must ensure that potentially privacy inferring information is obfuscated from the metadata. Two IF deployment options are considered with different impacts on security and especially privacy protection jurisdictions between IF and pilot ecosystems: 1. IF hosted on the project cloud (recommended for testing purposes and using test data for debugging and support) – integrators must ensure data anonymization at the northbound interface of services and IF must not store or process any privacy sensitive data that cannot be anonymized based on use case requirements; 2. IF hosted on integrator's resources (e.g., cloud platform of one of the pilot partners) so that integrator is in full control of security and privacy features (recommended for production deployment for full privacy protection control and managed scalability).

SPPs of the pilots are working, live documents. As the use cases are being implemented and new relationships established, the management plans will evolve. Business and exploitation potential of the pilots and their results directly depend on properly executed SPPs. The project tasks responsible for monitoring pilot execution will assess SPPs in different stages of their development. 3<sup>rd</sup> parties looking to join specific pilots (e.g., through cascaded funding) will have to comply to SPPs and management plans before integration into the semantically interoperable ecosystem.

Pilot SPPs are based on documented SPP, security threats, risks and measures of the IF. All project pilots, except Germany pilot Norderstedt location, utilize IF and rely on its SPP and threat analysis as the basis for building their own SPPs and conducting threat and risks analysis. Pilots introduce new security and data protection capabilities relying on the participating digital platforms. Regarding the actionable measures to be taken, pilots using IF will apply all IF measures, while introducing additional measures rising from specifics of participating digital platforms and use case requirements. The most important security measures are always the ones to secure the network and secure the data exchange along the network (e.g., Firewall, authentication, VPN). These capabilities are reinforced with access restrictions and user access management (including physical access control and restrictions). The privacy preserving measures are oriented to anonymize and unlink the PDL (Point de livraison – Point of Delivery like smart meter) from the data subject.

It is important to note that the SPP drafting process in each pilot involved multidisciplinary teams of security experts/engineers, data protection officers, decision makers and business strategists from organizations comprising the pilot ecosystems. The templates and methodology had to address this fact so that all relevant inputs are properly collected and integrated into the SPPs. An actionable SPP is not just a cybersecurity plan for the engineers, it also impacts organizational decisions and policy settings as the basis for establishing interoperable cross domain ecosystems (like project pilots).

The complete methodology, templates and lessons learned from the SPP drafting process can be exploited outside of the project itself. The methodology is presented in public deliverables where empty templates are documented as well as proper execution process. The pilot and

interoperability framework SPPs can be used as examples. The methodology is specifically well tailored for all projects and initiatives that call for establishing system of systems. During the project lifetime the SPPs and the methodology will be validated in its ability to setup, guide and maintain security and privacy aspects of large-scale cross domain pilots. All future Horizon projects tackling the challenges of cross domain interoperability and ecosystem building (system of systems) can apply the methodology documented in this (and other) project deliverables.

Finally, properly executed SPPs are empowering all ecosystem stakeholders including end users. The plans put specific focus on data and privacy protection in cross domain interoperable ecosystems. A well-executed and maintained SPPs ensure that end user privacy protection is always at the forefront of decision-making process and all ecosystem evolutions do not impact the set level of privacy protection.

# TABLE OF CONTENTS

---

ABSTRACT	4
EXECUTIVE SUMMARY	5
LIST OF FIGURES	14
LIST OF TABLES	15
ABBREVIATIONS AND ACRONYMS	17
1. INTRODUCTION	19
1.1 WP5 OBJECTIVES	19
1.2 RELATION TO OTHER WPS	19
1.3 D5.3 OBJECTIVES AND APPROACH	20
1.4 SECURITY AND PRIVACY PLAN	23
1.4.1 GOVERNANCE MANAGEMENT PLAN	23
1.4.2 DATA MANAGEMENT PLAN	23
1.4.3 RISK MANAGEMENT PLAN	24
1.4.4 ENGINEERING MANAGEMENT PLAN	24
1.4.5 CITIZEN MANAGEMENT PLAN	24
1.5 SECURITY AND PRIVACY ANALYSIS	24
1.6 DOCUMENT STRUCTURE	26
2. INTERCONNECT INTEROPERABILITY FRAMEWORK	27
2.1 SAREFIZATION PROCESS	29
2.2 SECURITY AND PRIVACY CAPABILITY OF THE INTERCONNECT INTEROPERABILITY FRAMEWORK	32
2.2.1 DEPLOYMENT CONSIDERATIONS	34
2.2.2 SCENARIO 1: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS AND GENERIC ADAPTERS IN SERVICES DOMAIN	34
2.2.3 SCENARIO 2: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS AND GENERIC ADAPTERS IN SERVICE AND INTERCONNECT CLOUD DOMAIN	35
2.2.4 SCENARIO 3: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS, KNOWLEDGE ENGINE INSTANCE AND GENERIC ADAPTERS IN SERVICE DOMAIN	36
2.2.5 CYBERSECURITY AND PRIVACY PROTECTION IN P2P MARKETPLACES	37
2.2.6 RELATIONSHIP WITH PILOT SECURITY AND PRIVACY	39
2.2.7 CHARACTERISATION OF THE INTERCONNECT INTEROPERABILITY FRAMEWORK	40
2.2.8 BUSINESS AND CONTRACTUAL CYBERSECURITY CAPABILITIES OF THE INTEROPERABILITY FRAMEWORK	42

2.2.9	TYPICAL SECURITY AND PRIVACY THREATS FOR INTERCONNECT INTEROPERABILITY FRAMEWORK	43
2.2.10	BREACHES AND IMPACT FOR INTERCONNECT INTEROPERABILITY FRAMEWORK	46
2.2.11	MEASURES FOR INTERCONNECT INTEROPERABILITY FRAMEWORK	47
2.3	INTEROPERABILITY FRAMEWORK SPP	50
3.	PILOTS IN BELGIUM	58
3.1	NANOGRID KOBEGEM (LED BY: THINK-E)	58
3.1.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	58
3.2	CORDIUM HASSELT (LED BY: VITO)	59
3.2.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	60
3.3	THOR PARK GENK (LED BY: VITO)	62
3.3.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	62
3.4	STUDENTS ROOMS TOWER ANTWERP (LED BY: IMEC)	63
3.4.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	64
3.5	SMART DISTRICT NIEUWE DOKKEN GENT (LED BY: DUCOOP)	65
3.5.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	65
3.6	ZELLIK GREEN ENERGY PARK BRUSSELS (LED BY: VUB)	67
3.6.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	67
3.7	OD-HEVERLEE PUBLIC BUILDINGS (LED BY: 3E)	68
3.7.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	69
3.8	MECHELEN (LED BY: THERMOVULT)	70
3.8.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	71
4.	GREEK PILOT	72
4.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	72
5.	DUTCH PILOT	74
5.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	74
6.	FRENCH PILOT	77
6.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	78
7.	PORTUGUESE PILOT	80
7.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	81
8.	ITALIAN PILOT	83
8.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	83
9.	CROSS-BORDER INTEROPERABILITY PILOT	86
9.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	86

10.	GERMAN PILOTS	88
10.1	NORDERSTEDT LOCATION	88
10.1.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	89
10.2	HAMBURG LOCATION	90
10.2.1	ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS	91
11.	CROSS ANALYSIS OF PILOTS	93
12.	CONCLUDING REMARKS	97
	REFERENCES	101
	ANNEX 1. GUIDELINES USED TO CARRY OUT THE SECURITY AND PRIVACY RISK ANALYSIS OF INTERCONNECT PILOTS	102
	ANNEX 1.1 THREAT IDENTIFICATION: STRIDE AND LINDDUN TABLES	102
	ANNEX 1.2 IMPACT ASSESSMENT GUIDELINE: RISK MODEL AND RISK MAP	103
	ANNEX 1.3 EXAMPLES OF BREACH IMPACT	104
	ANNEX 1.4 CONTROL CATEGORIES	105
	ANNEX 2. SECURITY AND PRIVACY PLANS PER PILOT	106
	ANNEX 2.1 PILOTS IN BELGIUM: SPP	106
	ANNEX 2.1.1 NANOGRIID KOBEGEM (THINK-E)	106
	ANNEX 2.1.2 CORDIUM HASSELT (VITO)	109
	ANNEX 2.1.3 THOR PARK GENK (VITO)	113
	ANNEX 2.1.4 STUDENTS ROOMS TOWER ANTWERP (IMEC)	116
	ANNEX 2.1.5 SMART DISTRICT NIEUWE DOKKEN GENT (DULOOP)	120
	ANNEX 2.1.6 ZELLIK GREEN ENERGY PARK BRUSSELS (VUB)	125
	ANNEX 2.1.7 OUD-HEVERLEE PUBLIC BUILDINGS (3E)	128
	ANNEX 2.1.8 MECHELEN (THERMOVULT)	133
	ANNEX 2.2 GREEK PILOT SPP	136
	ANNEX 2.3 DUTCH PILOT SPP	145
	ANNEX 2.4 FRENCH PILOT SPP	154
	ANNEX 2.5 PORTUGUESE PILOT SPP	169
	ANNEX 2.6 ITALIAN PILOT SPP	175
	ANNEX 2.7 CROSS-BORDER INTEROPERABILITY PILOT SPP	181
	ANNEX 2.8 GERMAN PILOTS SPP	184
	ANNEX 2.8.1 NORDERSTEDT LOCATION (EEBUS)	184
	ANNEX 2.8.2 HAMBURG LOCATION (KEO-CONNECTIVITY)	187

## LIST OF FIGURES

FIGURE 1 - RELATION OF WP5 TO OTHER WPS	20
FIGURE 2: DELIVERABLES AND SCHEDULE OF EXPECTED OUTCOMES	22
FIGURE 3: PLANS TO BE DEFINED WITHIN THE SPP	24
FIGURE 4: INTERCONNECT INTEROPERABILITY FRAMEWORK - HIGH LEVEL ARCHITECTURE	27
FIGURE 5: INTEROPERABILITY FRAMEWORK INTERFACES AND DIVISION OF SECURITY AND PRIVACY PROTECTION RESPONSIBILITY BETWEEN FRAMEWORK AND PILOT ECOSYSTEM	28
FIGURE 6 - SAREFIZATION PROCESS	29
FIGURE 7: SYSTEM OF SYSTEM VISION	30
FIGURE 8: SYSTEM OF SYSTEM EMERGING RISK	31
FIGURE 9 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 1	34
FIGURE 10 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 2	35
FIGURE 11 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 3	36
FIGURE 12 - RELATION BETWEEN PILOT SPP AND INTEROPERABILITY FRAMEWORK SPP	40
FIGURE 13: OVERVIEW OF THE NANOGRIID KOBEGEM PILOT	106
FIGURE 14: DATA FLOW DIAGRAM FOR PILOT NANOGRIID KOBEGEM	108
FIGURE 15: OVERVIEW OF CORDIUM HASSELT PILOT ARCHITECTURE	110
FIGURE 16: OVERVIEW OF THE THOR PARK GENK PILOT ARCHITECTURE	113
FIGURE 17: OVERVIEW ARCHITECTURE OF STUDENTS ROOMS TOWER ANTWERP PILOT	117
FIGURE 18: DATA FLOW DIAGRAM OF STUDENTS ROOMS TOWER ANTWERP PILOT	119
FIGURE 19: DATA ACCESS DIAGRAM	119
FIGURE 20: OVERVIEW ARCHITECTURE OF NIEUWE DOKKEN GENT PILOT	121
FIGURE 21: DATA FLOW DIAGRAM NIEUWE DOKKEN GENT PILOT	123
FIGURE 22: DATA ACCESS DIAGRAM NIEUWE DOKKEN GENT PILOT	124
FIGURE 23: OVERVIEW ARCHITECTURE OF ZELLIK GREEN ENERGY PARK PILOT	125
FIGURE 24: OVERVIEW ARCHITECTURE OF OUD-HEVERLEE PUBLIC BUILDINGS PILOT	129
FIGURE 25: DIAGRAM OF DATA FLUX OF OUD-HEVERLEE PILOT	129
FIGURE 26: OVERVIEW ARCHITECTURE MECHELEN PILOT	133
FIGURE 27: OVERVIEW ARCHITECTURE OF GREEK PILOT	137
FIGURE 28: DATA FLOW DIAGRAM GREEK PILOT	142
FIGURE 29: DATA ACCESS DIAGRAM GREEK PILOT	143
FIGURE 30: GENERAL OVERVIEW DIAGRAM OF DUTCH PILOT	145
FIGURE 31: HIGH-LEVEL OVERVIEW OF SYSTEMS COMPONENTS	146
FIGURE 32: DATA FLOW AND SPECIFICATION OF DUTCH PILOT	149
FIGURE 33: DATA FLOW DIAGRAM OF DUTCH PILOT	150
FIGURE 34: DATA ACCESS CONTROL CHART OF DUTCH PILOT	150
FIGURE 35: OVERVIEW ARCHITECTURE OF FRENCH PILOT	154
FIGURE 36: DATA FLOW DIAGRAM OF ENGIE DATA	161
FIGURE 37: OVERVIEW ARCHITECTURE OF PORTUGUESE PILOT	170
FIGURE 38: OVERVIEW ARCHITECTURE OF ITALIAN PILOT	175
FIGURE 39: OVERVIEW ARCHITECTURE OF CROSS-BORDER PILOT	182
FIGURE 40 SIMPLIFIED OVERVIEW OF THE CROSS-BORDER PILOT	182
FIGURE 41: OVERVIEW ARCHITECTURE OF GERMAN PILOT IN NORDERSTEDT	184
FIGURE 42: OVERVIEW ARCHITECTURE OF GERMAN PILOT IN HAMBURG	187

## LIST OF TABLES

TABLE 1 - SPP CAPABILITIES AND DESCRIPTIONS .....	25
TABLE 2 - SPP CAPABILITIES AND DESCRIPTIONS .....	25
TABLE 3 - CHARACTERISTICS OF THE INTEROPERABILITY FRAMEWORK .....	42
TABLE 4 - INTERCONNECT INTEROPERABILITY FRAMEWORK BUSINESS AND CONTRACTUAL CYBERSECURITY CAPABILITIES .....	42
TABLE 5 - THREATS FOR INTERCONNECT INTEROPERABILITY FRAMEWORK .....	43
TABLE 6 - THREATS FOR THE INTEROPERABILITY FRAMEWORK .....	45
TABLE 7 - THREATS FOR PILOTS USING THE INTERCONNECT INTEROPERABILITY .....	46
TABLE 8 - BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK.....	46
TABLE 9 - THREATS THAT CAN CAUSE BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK .....	46
TABLE 10 – IMPACT FROM BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK.....	47
TABLE 11 - MEASURES IN INTERCONNECT INTEROPERABILITY FRAMEWORK.....	48
TABLE 12 - RELATIONSHIP BETWEEN MEASURES AND IDENTIFIED THREATS IN THE INTERCONNECT INTEROPERABILITY FRAMEWORK .....	49
TABLE 13 - CHARACTERISATION OF NANOGRID KOBEGEM PILOT .....	58
TABLE 14 PILOT CYBERSECURITY CAPABILITIES OF THE NANOGRID KOBEGEM PILOT.....	59
TABLE 15 CHARACTERIZATION OF CORDIUM HASSELT PILOT .....	60
TABLE 16 CYBERSECURITY CAPABILITIES OF CORDIUM HASSELT PILOT.....	60
TABLE 17 - DIGITAL PLATFOMS PARTICIPATING IN THE CORDIUM HASSELT PILOT .....	60
TABLE 18 CHARACTERISATION OF THOR PARK GENK PILOT.....	62
TABLE 19 CYBERSECURITY CAPABILITIES OF THOR PARK GENK PILOT .....	63
TABLE 20 CHARACTERISATION OF THE STUDENTS' ROOMS TOWER ANTWERP PILOT.....	63
TABLE 21 CYBERSECURITY CAPABILITIES OF THE STUDENT'S ROOMS TOWER ANTWERP PILOT .....	64
TABLE 22 - DIGITAL PLATFORM PARTICIPATING IN THE STUDENT'S ROOMS TOWER ANTWERP PILOT .....	64
TABLE 23 CHARACTERISATION OF DE NIEUWE DOKKEN PILOT .....	65
TABLE 24 CYBERSECURITY CAPABILITIES OF DE NIEUWE DOKKEN PILOT.....	65
TABLE 25 - DIGITAL PLATFORM PARTICIPATING IN DE NIEUWE DOKKEN PILOT.....	65
TABLE 26 CHARACTERISATION OF THE ZELLIK GREEN ENERGY PARK BRUSSELS PILOT .....	67
TABLE 27 CYBERSECURITY CAPABILITIES OF ZELLIK GREEN PARK ENERGY PILOT .....	68
TABLE 28 CHARACTERISATION OF THE OUD-HEVERLEE PILOT .....	69
TABLE 29 CYBERSECURITY CAPABILITIES OF THE OUD-HEVERLEE PILOT.....	69
TABLE 30 - DIGITAL PLATFORM PARTICIPATING IN THE OUD-HEVERLEE PILOT .....	69
TABLE 31 CHARACTERIZATION OF MECHELEN PILOT .....	71
TABLE 32 - DIGITAL PLATFORM PARTICIAPTING IN THE MECHELEN PILOT .....	71
TABLE 33 CHARACTERISATION OF THE GREEK PILOT .....	72
TABLE 34 CYBERSECURITY CAPABILITIES OF GREEK PILOT.....	72
TABLE 35 - DIGITAL PLATFORMS PARTICIPATING IN THE GREEK PILOT .....	73
TABLE 36 CHARACTERISATION OF THE DUTCH PILOT .....	74
TABLE 37 CYBERSECURITY ADDITIONAL CAPABILITIES OF THE DUTCH PILOT.....	74
TABLE 38 - DIGITAL PLATFORMS PARTICIPATING IN THE DUTCH PILOT .....	75
TABLE 39 CHARACTERISATION OF THE FRENCH PILOT .....	77
TABLE 40 CYBERSECURITY CAPABILITIES OF THE FRENCH PILOT .....	78
TABLE 41 - DIGITAL PLATFORMS PARTICIPATING IN THE FRENCH PILOT.....	78
TABLE 42 CHARACTERIZATION OF PORTUGUESE PILOT .....	80



TABLE 43 CYBERSECURITY CAPABILITIES OF THE PORTUGUESE PILOT .....	81
TABLE 44 - DIGITAL PLATFORMS PARTICIPATING IN THE PORTUGUESE PILOT.....	81
TABLE 45 CHARACTERIZATION OF THE ITALIAN PILOT.....	83
TABLE 46 CYBERSECURITY CAPABILITIES OF THE ITALIAN PILOT.....	84
TABLE 47 - DIGITAL PLATFORM PARTICIPATING IN THE ITALIAN PILOT.....	84
TABLE 48 CHARACTERISATION OF CROSS-BORDER PILOT .....	86
TABLE 49 CYBERSECURITY CAPABILITIES OF THE CROSS-BORDER PILOT .....	86
TABLE 50 - DIGITAL PLATFOM OF THE CROSS-PILOT SCENARIO .....	86
TABLE 51 CHARACTERISATION OF THE NORDERSTEDT PILOT .....	88
TABLE 52 CYBERSECURITY CAPABILITIES OF THE NORDERSTEDT PILOT.....	89
TABLE 53 CHARACTERIZATION OF THE HAMBURG PILOT .....	91
TABLE 54 CYBERSECURITY CAPABILITIES OF THE HAMBURG PILOT .....	91
TABLE 55 - DIGITAL PLATFORMS PARTICIPATING IN THE GERMAN PILOT - HAMBURG LOCATION .....	91
TABLE 56 SECURITY AND PRIVACY CROSS ANALYSIS OF PILOTS.....	95
TABLE 57 - OVERVIEW OF COMPLETENESS OF PILOTS' SPPS AS PRESENTED IN THIS DELIVERABLE .....	99
TABLE 58: STRIDE SECURITY THREATS CATEGORIES .....	102
TABLE 59: LINDDUN PRIVACY THREATS CATEGORIES .....	103
TABLE 60: RISK MAP .....	104
TABLE 61: IMPACT EXAMPLES .....	104
TABLE 62: CONTROL CATEGORIES .....	105

## ABBREVIATIONS AND ACRONYMS

AC	Alternate Current
A/C	Alternate/Continuous
AES	Advanced Encryption Standard
aFRR	Automatic Frequency Restoration Reserves
API	Application Programming Interface
App	Application
B_IF	Breach Interoperability Framework
BSI	Britain Standards Institution
BTES	Borehole Thermal Energy Storage
CEN-CENELEC	Comité Européenne de Normalisation en Electronique et en Electrotechnique
CO	Carbon monoxide
CO <sub>2</sub>	Carbon dioxide
CLS	Communication Lionbrige Switzerland
CMMI	Capability Maturity Model Integration
CNIL	Commission Nationale de l'Informatique et Libertés
CTO	Chief Technology Officer
DC	Direct Current
DCM BEM	Block Element Modifier
DER	Distributed energy resource
DHW	Domestic Hot Water
DoS	Denial of Service
DR	Demand Response
DPIA	Data Privacy Impact Assessment
DSF	Double Skin Façade
DSO	Distribution System Operator
EU	Europe
EMS	Electric Mobility System
ENISA	European Union Agency for Cybersecurity
EV	Electrical Vehicle
FSP	Flexibility Service Provider
GA	Grant Agreement
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HLUC	High Level Use Case
HP	Heat pump
HVAC	High Voltage Alternate Current
IaaS	Infrastructure as a Service
IF	Interoperability Framework
ICT	Information Communication Technologies
ISO/IEC	International Standard Organisation/International Electrotechnical Commission
IDP	IDentity Provider
IEMS	Integrated Energy Management System
IoT	Internet of Things
I/O	In/Out
IP	Internet Protocol
JSON	JavaScript Object Notation
kWh	Kilowatt Hour
LCOE	Levelized Cost of Energy

LINDDUN	Linkability Identifiability Non-repudiation Detectability Disclosure of information Unawareness Non-compliance
LV	Low Voltage
M_IF	Measures_Interoperability Framework
mFRR	Manual Frequency Restoration Reserves
MoM	Minutes of meetings
NH3	Ammoniac
NIST	National Institute of Standards and Technology
N/A	Not Applicable
OCP	Open Charge Point Protocol
PaaS	Platform as a Service
PC	Personal Computer
PDL	Point de Livraison PoD
PII	Personal Information Identifiable
PIMS	Privacy Information Management System
PIR	Passive Infrared System
POC	Point of Contact
PoD	Point of Delivery
PUC	Pilot Use Case
PTU	Program Time Unit
PV	PhotoVoltaic
PVT	PhotoVoltaic Thermal
P2P	Peer to Peer
Q	Quarter
RES	Renewable Energy Sources
R&D	Research and Development
SAREF	Smart Applications REference
SGE	Système de gestion des échanges
SIL	Semantic Interoperability Layer
SLT	Senior Leadership Team
SME	Small Medium Enterprise
SO	Smart Orchestrator
SoS	System of Systems
SPOCS	Security and Privacy Policies cOmpliance Solutions
SPP	Security and Privacy Plan
SQL	Structure Query Language
STRIDE	Spoofing Tampering Repudiation Information Disclosure Denial of service Elevation of privilege
SSL	Secure Sockets Layer
T	Task
TDE	Transparent Data Encryption
T-EMS	Transport Energy Management System
TIC	Technologies de l'Information et de la Communication (ICT in English)
T_IF	Threat Interoperability Framework
TLS	Transport Layer Security
TSO	Transmission System Operator
UTF	Universal character set Transformation Format
WP	Work Package
W3C	World Wide Web Consortium
W/h	Watt/hour

## 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);
- Lastly, provide a description of the platforms, devices, and services to be exploited in WP7 (T5.5).

This WP is responsible for delivering **InterConnect Interoperability Framework (IF)** 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 will support 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 back to those 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 Distribution System Operator (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 Interoperability Framework toolbox necessary for making their platforms and services interoperable with the Interoperability Framework and established pilots.

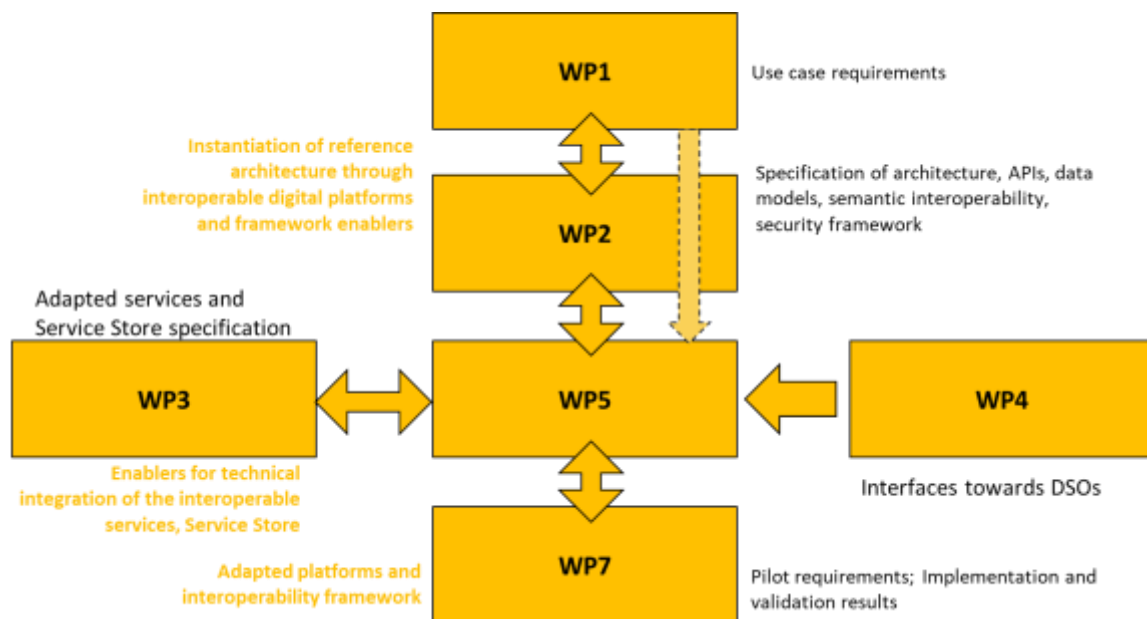


FIGURE 1 - RELATION OF WP5 TO OTHER WPS

## 1.3 D5.3 OBJECTIVES AND APPROACH

Deliverable 5.3 presents the work done until M24 in actionable security and privacy management practices within the pilots and the InterConnect interoperability framework. Its main objectives can be detailed as follows:

- An introduction to the security and privacy management practice applied within the pilots and the InterConnect interoperability framework: the Security and Privacy Plan (SPP) and the security and privacy risk analysis.
- The results of the security and privacy risk analysis of the InterConnect interoperability framework and the pilots.
- A cross-analysis of the pilots' risk analysis on the security and privacy practice activity applied within the project.

The InterConnect project aims to provide an efficient energy management through a flexible and interoperable ecosystem where demand flexibility could be integrated with comfort and convenience for end-users. Semantic interoperability is at the project's core. **The InterConnect interoperability framework** is designed and implemented so that it enables

tangible semantic interoperability between services, digital platforms, devices, and applications which are comprising the project pilots and their use cases. The project includes 7 large scale pilot and one overarching use case for flexibility management (see deliverable D1.1 [6] for details).

Each large-scale pilot represents an ecosystem where different actors are involved, collecting and sharing data between services. Each pilot envisions a set of use cases. Use cases translate into different set of requirements for security and privacy protection.

Each pilot must therefore integrate the ecosystem vision in the management of security and privacy. The need to have an ecosystem perspective is exemplified in ISO/IEC 27570 (privacy guidelines for smart cities). Deliverable D2.2 [1] (section 3.1.1) makes the point that there are no known practices on ecosystem security and privacy plans (SPPs). Therefore, InterConnect promotes the following building blocks:

- A **common practice** for security and privacy plans in project pilots.
- The **use of a common** building block, the **InterConnect Interoperability Framework**, which includes security and privacy management capabilities.

Figure 2 shows the role of Task T5.3 and deliverable D5.3:

- T5.3 is responsible for the specification of the pilots SPPs as well as the specification of supporting material related to the use of the InterConnect interoperability framework.
- D5.3 is the outcome of task T5.3. It is based on deliverable D2.2 (Privacy and Security Design Principles and Implementation Guidelines), which is the outcome of task T2.3. Deliverable D2.2 specifies two practices, the SPP practice and the Policy framework analysis. The SPP includes 5 elements: governance, risk management, data management, engineering management and citizen engagement management. The policy framework analysis aims to give a final analysis of the pilot implementation and provide feedback at policy level.

The approach considers a series of strategic meetings to accommodate the SPP as a living document, namely:

- **m1**: organized as a webinar explaining the principles and goals of the creation of a SPP.
- **m2**: organized as individual workshops with pilots' partners focused on explaining the content of the SPP and to support its development (in task T5.3 and in context of the pilot).

As pilots implement the SPP, subsequent strategic meetings are organized, namely:

- **IF**: this meeting is organized with the InterConnect Interoperability framework developers and maintainers. It kicks-off the contribution of the InterConnect IF to the security privacy risk analysis, so that it can be used as basis by the pilots.
- **m3**: a series of meetings that focused on pilots' SPP evolution with security and risk analysis based on the InterConnect IF security and privacy risk analysis.

Each pilot SPP is an individual living document that will be maintained internally by the pilots' team starting in the fourth quarter of 2021. At the end of the project, pilots will provide feedback

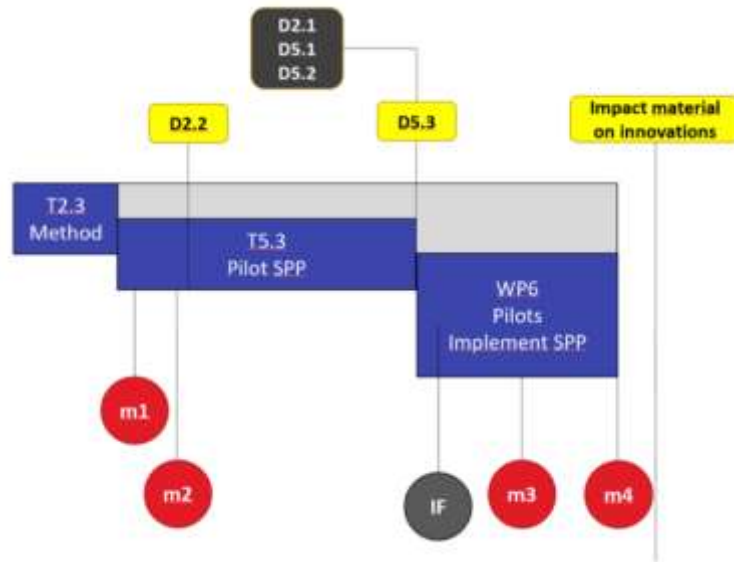
based on their experience in the application of the SPP during the implementation, which will be addressed in the final strategic meeting to be conducted in the scope of WP6 and WP7:

- **m4:** exchange impressions and information from their experience to build a policy framework analysis for each pilot. The approach is to collect information about issues faced, recommendations and best practices to apply in similar pilots and environments which will continue implementing and maintaining the InterConnect technologies after the project. An analysis from a trust view of socio-economic and business perspective is expected as well as on ethics and standardization. Final documentation of the pilot SPPs will be delivered by corresponding WP7 tasks.

During the project, impact material on innovation will be collected. For instance, the return from experience provided by the policy framework analysis could be used as innovation material for support actions or body of knowledge (e.g., standardization).

As the InterConnect pilots may have different objectives and priorities, and have different status, it is important to point out the following:

- An SPP might include entries that are not relevant to certain pilots. Further, some entries might not be relevant in the frame of the pilot but will be relevant beyond for exploitation. Some entries can therefore be marked as “not relevant in the pilot”.
- The security and privacy plan might include entries that are not finalized yet, as it can depend on decisions that are taken later in the development. Some entries could therefore be marked as “to be specified” (TBS).



**FIGURE 2: DELIVERABLES AND SCHEDULE OF EXPECTED OUTCOMES**

The pilot SPPs will provide inputs for the project level data management plan (also a living document and process maintained on the project level). The data management plan will have references towards the pilot SPPs. The main decisions of the project data protection officers will impact SPP maintenance.



## 1.4 SECURITY AND PRIVACY PLAN

---

The SPP is the first practice identified for ICT ecosystems. The goal is that it provides methods and tools to define the actions, guidelines to follow-up to manage, analyse and treat security and privacy risks and challenges. At the end, this document will help to define technical and management solutions to cybersecurity and privacy risks.

It is a living document that is updated along the project and beyond the project, in the future exploitation. There are scheduled internal pilot meetings, where the security and privacy are topics to analyse. One of the points is always to review the actions planned in each part of the SPP and integrate them. The pilot manager should reflect any change in the principal parts of the plan, such as

- Changes in the data flow of the system should be reflected and discussed to undergo any required update actions (e.g., need of agreements, roles of data processors, collectors).
- Organisational changes, from an engineering point of view in the development of the system or the privacy engineering practice to undergo any required updates.

All SPP versions and revisions must be kept, to evaluate the changes and progresses throughout time.

This plan provides an operational analysis of each pilot. The implementation of this plan is structured in 6 parts described in the ISO/IEC 27570 ecosystem privacy plan, which has been taken as its, extending to include security. Thus, 5 different subplans are meant to be provided according to Figure 3, as described in the following paragraphs.

### 1.4.1 GOVERNANCE MANAGEMENT PLAN

---

Governance is the first step to provide a proper SPP and a proper application of it. In this part three main things must be detailed:

- The rules, laws, standards, and norms that are meant to be accomplished and followed within the SPP for that pilot or ecosystem. That is, the specification from high-level legislation, which today in Europe is the GDPR to the specific standards that are followed (i.e., for defining use cases).
- The main roles, committee, and organisation structure. A DPO must be nominated as a contact point for any question about Data protection and flow and for accountable technical system(s).
- Continuous improvement (committee). A committee should be in place to assess and improve any issues surrounding services, providing a better security and privacy protection within the system, during and beyond the duration of the project in the exploitation phase.

### 1.4.2 DATA MANAGEMENT PLAN

---

The data management plan takes its basis from the Data Management Plan of the project, specifying in detail the data flow of the ecosystem in each pilot; the data sets collected and treated, who will be the collector and the processor, the procedures and the registry of different

consents and treatments done. This configures a very important part of the SPP, as it clearly describes the data, its flow and usage. Moreover, it specifies the different agreements between entities that are sometime needed to prevent data sharing beyond the agreed terms.

### 1.4.3 RISK MANAGEMENT PLAN

---

The Risk Management Plan depicts the contexts in which the security and privacy analysis are conducted within the pilot ecosystem and which methods will be chosen to be applied during the security and privacy risk analysis. It depends on the countries and the needs of the ecosystem.

### 1.4.4 ENGINEERING MANAGEMENT PLAN

---

Privacy-by-design is one of the main topics of privacy during the last years and it is taking more and more importance in the engineering process and work as it is becoming essential the integration of privacy within all the lifecycle of the engineering process. The Engineering Management Plan translates into the different techniques, standards, methods, and guidelines that each entity and within the ecosystem can follow to enhance the security and privacy. In this subplan, all these methods, guidelines or standards used are specified.

### 1.4.5 CITIZEN MANAGEMENT PLAN

---

This plan is linked to the citizen engagement and citizen rights such as transparency, in the case of privacy. All the activities, documents prepared to clarify the citizens their role, their data usage, for what purposes, its rights to withdraw are essential to create awareness but also trustworthiness in the business and the stakeholders from them.



**FIGURE 3: PLANS TO BE DEFINED WITHIN THE SPP (THE SAME COLOR CODING IS APPLIED IN THE SPP TABLES OF IF AND PROJECT PILOTS IN ANNEXES)**

The detailed information about the implementation of these plans and templates provided are already explained in D2.2, sections 3.2 and 4.2 [1].

## 1.5 SECURITY AND PRIVACY ANALYSIS

---

The step to establish a security and privacy practice under an ecosystem view is to perform the security and privacy risk analysis (defined as **m3**).

It is important to highlight that the risk management should be continuous, as the assessment should be conducted several times in different phases of the lifecycle of a project or periodically within an organisation, to perform risk analysis, for example. In the case of the InterConnect, pilots are not fully deployed, therefore the security and privacy analysis, as well as the SPP will be updated.

Focusing on the Security and privacy risk analysis, T5.3 team has performed two dedicated workshops with each pilot. These workshops have explained the process and how to carry out the security and privacy risk analysis. For this purpose, it has been presented an internal template report to fulfil after the risk analysis. The security and privacy risk analysis performed by the InterConnect interoperability framework serves as a base for most of the pilots as technology adopters.

For each pilot, a summary of the pilot organization and the principal cybersecurity capabilities are presented in this report (see Table 1). The characterisation of the pilot briefly details the actors involved, the use cases that the pilot carries out and the architecture entities that encompasses the pilot.

<b>Actors</b>	list the actors	Brief description of their role and functions.
<b>Use cases</b>	list the use cases	Brief description of each one.
<b>Architecture entities</b>	list the entities, where the Interoperability framework is almost always	Brief description of the function in the pilot of each one.

**TABLE 1 - SPP CAPABILITIES AND DESCRIPTIONS**

After the characterisation of the pilot, cybersecurity capabilities of the pilot as a system of systems will be summarized as shown in Table 2.

<b>Capabilities</b>	<b>Description</b>
list available capabilities and specific actions to enable them	Brief description of the capability implemented

**TABLE 2 - SPP CAPABILITIES AND DESCRIPTIONS**

Once the pilot or the system (as it has been used by the Interoperability framework analysis) is described, identified system breaches are documented (description and impact indicators from minor over significant to maximum).

A breach in a system or in an organisation is a release (intentional or not) of private and secure data or information to an untrusted environment. A data breach is a security violation of data that is accessed, copied, transmitted, stolen, used, viewed by an authorized individual. It is the consequence of an incident that compromises the system.

If there is a breach, the causes of the cybersecurity incident must be identified to be addressed with improved security and privacy within the system. This cybersecurity incident or event is called a threat. To identify different threats, STRIDE and LINDDUN (see Annex 1.1) methods are used by the pilots. The first one more oriented to security and the second one to privacy. Pilots and interoperability framework development team have analysed the possible threats category by category, and they have been listed in the corresponding tables. As said before, the interoperability framework as a toolset for pilots requires its own threat analysis table and the links to threats and breaches as causes. Consequences are taken as a reference by all the pilots. Pilots added, sometimes, more threats complementing the ones provided by the

Interoperability framework. These threats are inherent from the digital platforms and other digital systems comprising the pilots as well as from the new integration decisions made within the pilot teams.

Once the threats are identified and linked to the breaches, the risk that a threat can materialize into a breach are quantified. The risk is assessed using the calculation and table in Annex 1.2, where the scale of risk goes from Negligible to Maximum, after being multiplied by the likelihood to materialize by the impact. To clarify the impact of a breach in the ecosystem, we introduce a table where impact is split into perimeters:

- Ecosystem: the ecosystem reputation is evaluated as a whole.
- Organisations: the different organisations involved in the pilot are evaluated. The Interoperability framework and the pilot manager are always evaluated. But in some pilots, there are other organisations considered, such as technical provider.
- Citizen: In this case, the item to evaluate is their privacy which, for example, in a personal data breach or massive personal data breach will be of high impact.

The risk analysis of the incidents and how they materialize into a breach in the system is mapped using the table *risk map* of Annex 1.2.

Moreover, controls are classified as any measure or action that can modify the risk level. A classification system is available with categories and sub-categories specified in ISO 27701 and ISO 27002, both listed in Annex 1.4.

## 1.6 DOCUMENT STRUCTURE

---

This introduction is part of **Chapter 1**.

**Chapter 2 – InterConnect Interoperability Framework** addresses the construction of the interoperability framework by establishing and addressing the ICT and Data Privacy boundaries to be expected. At the same time, it highlights their implications to pilot deployments, considering the system-of-systems construct. Finally, it discussed the security, data privacy and cybersecurity capabilities the Interoperability Framework and its components.

**Chapter 3** – Introduces the general setup of risk and threat analysis procedure for each project pilot.

**Chapter 4 – 10** introduce analysis of security and privacy protection capabilities and risks for all project pilots.

**Chapter 11** - provides overall analysis of all pilots in a single table and introduces best practice recommendations to be considered by the project pilots.

**Chapter 12** - concludes the document.

Finally, the document includes **two Annexes** with the guidelines to conduct a security and privacy risk analysis (threats categories, example of breaches, impact risk scale and control categories) and the SPPs of the project pilots.

## 2. INTERCONNECT INTEROPERABILITY FRAMEWORK

Each InterConnect project pilot comprises a set of digital platforms, services, applications, devices, and other resources provided by participating partners. The overall action is based in the System of Systems approach. The main challenge behind the InterConnect project is to enable all these systems to be interoperable. To achieve this, the project introduces the **InterConnect Interoperability Framework** (Figure 4), which enables semantic interoperability for all participating digital platforms, providing access to energy and non-energy services (e.g., control, comfort, and convenience) and devices.

The central component is the semantic interoperability layer which interconnects existing digital platforms, and services they offer, together with the remainder interoperability framework enablers and capabilities including the service store, P2P marketplaces, compliance certification, data protection and access control and supporting services.

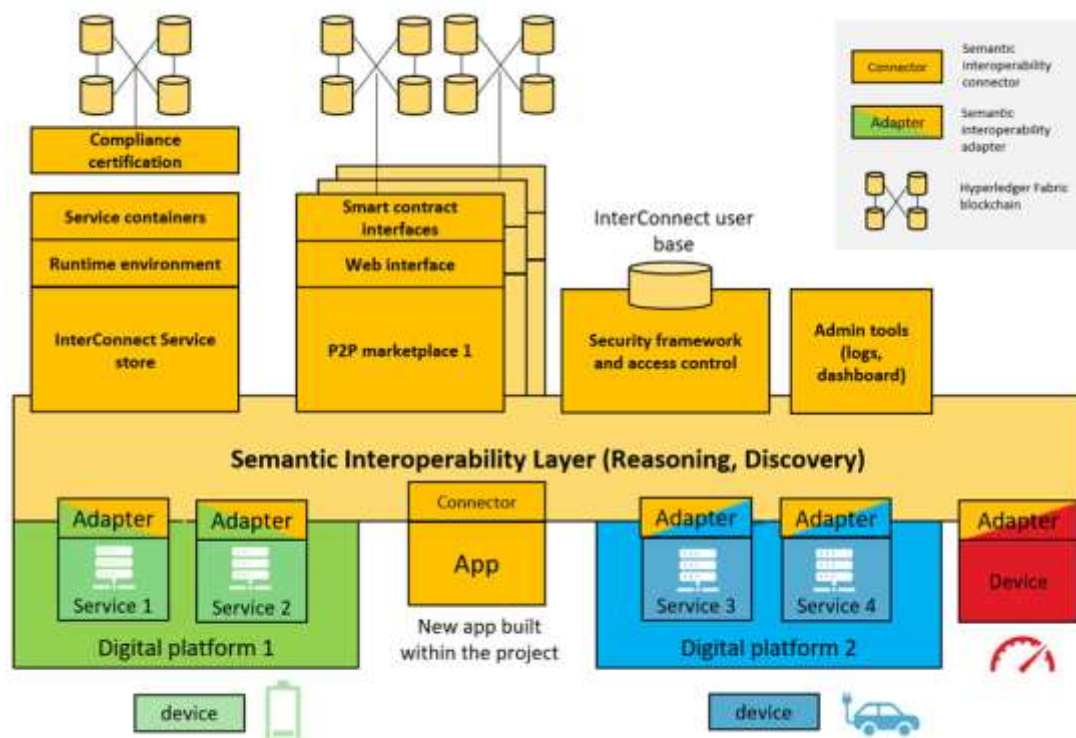


FIGURE 4: INTERCONNECT INTEROPERABILITY FRAMEWORK - HIGH LEVEL ARCHITECTURE

The **InterConnect interoperability framework** introduces the interoperability **Generic Adapters** as key enablers for digital platform operators and service providers to make their services and data endpoints interoperable according to the InterConnect approach (unified interfaces with focus on joint ontology). The **Generic Adapters** are responsible for (see Figure 5):

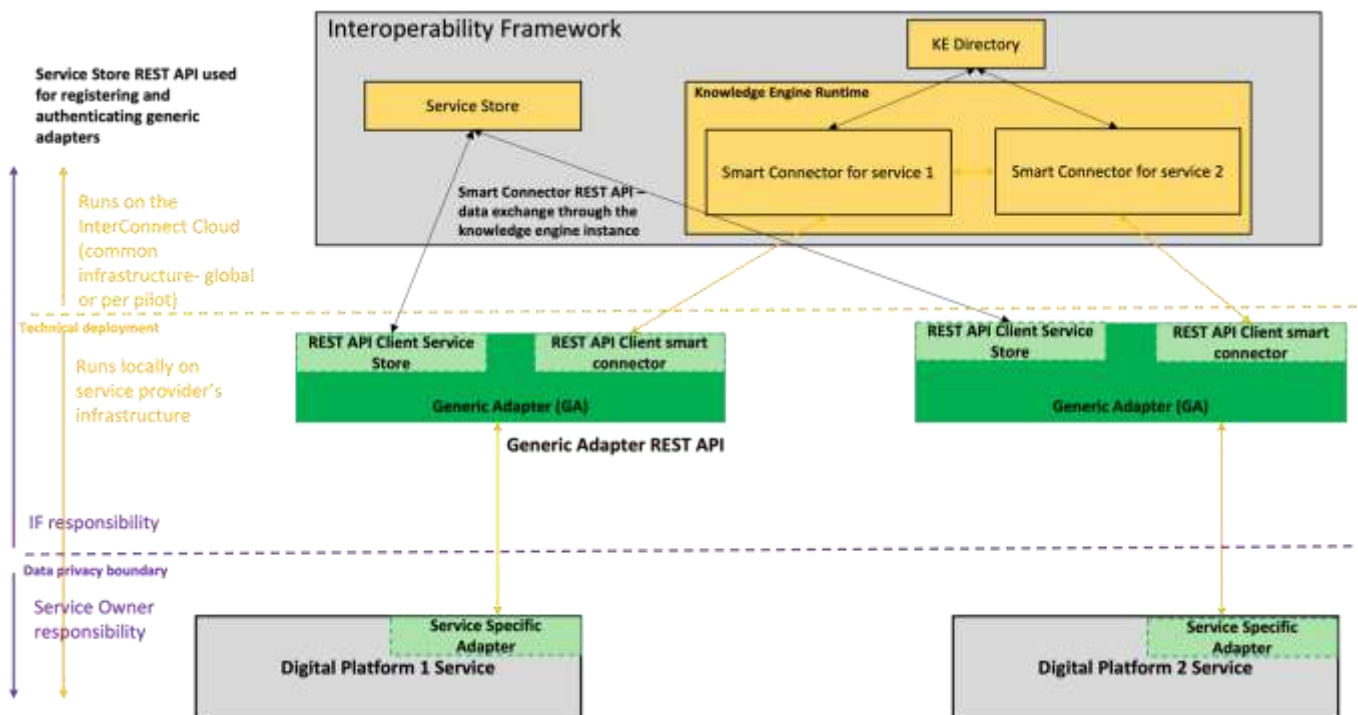
- Maintaining interface between services and the InterConnect Service Store. The Service Store provides catalogue of all registered interoperable services along with their characteristics. Through this interface, services are authorized to access and utilize the interoperability framework components and other interoperable services.



- Interfacing with the core services of the InterConnect interoperability layer for interoperable semantic data delivery. The InterConnect interoperability layer is based on the Knowledge Engine technology.
- Establishing data exchange channels between two or more instances of **Generic Interoperability Adapters** which serve specific services, applications, and devices.

The InterConnect interoperability framework does not store any operational data exchanged between services equipped with the interoperability adapters. The interoperability layer and service store manage metadata and service description data necessary for running semantic discovery and reasoning operations.

When it comes to the exchange of operational (potentially privacy sensitive) data, the interoperability adapters enable services to exchange data in interoperable manner. Services utilize their interoperability adapters to engage in semantic discovery and reasoning operation and once the required data endpoint or other service is identified, the data exchange channel is established between the two endpoints. Figure 5 showcases what is the data protection jurisdiction of the interoperability framework provider and project pilot which is instantiating the framework to enable semantic interoperability between subsystems of participating stakeholders.



**FIGURE 5: INTEROPERABILITY FRAMEWORK INTERFACES AND DIVISION OF SECURITY AND PRIVACY PROTECTION RESPONSIBILITY BETWEEN FRAMEWORK AND PILOT ECOSYSTEM**

It clearly highlights the two domains of interest for that discussion: **the ICT technical deployment** and the considered **data privacy boundary**.

Given this scenario, two main rules of thumb apply:

- **ICT technical deployment:** The location and hence the entity that is in control for the components themselves. Consider if a given component of the interoperability framework is deployed within the partner premises or in a foreign entity (e.g., within a public cloud provider).

- **Data Privacy boundary:** The need to realize the criticality of providing data as input to the interoperability framework and any needs/assurances of data protection/governance by a service before engaging with the Interoperability Framework.

Figure 5 realizes the interoperability framework along with both borders. It considers the standard deployment option, where service owners deploy the services in a domain controlled by them, together with their Service Specific Adapter and Generic Adapter. The common interoperability framework components such as the service store or the Knowledge Engine remain deployed in a cloud instance for the purpose of the project.

This provides separation regarding the governance responsibility of these components. While the common components, in this deployment option, are in control of the maintainers of the InterConnect cloud (hosted by INESC TEC – as September 2021, with components maintained by core T5.2 partners), the services themselves and the respective Service Specific Adapters and Generic Adapters are governed by the partners owning or responsible by the services. In terms of data privacy, services, service specific adapters and the considered Generic Adapter and the decisions to make data available through them is completely in the jurisdiction of partners responsible for those services.

That means that, the decision of what, when, with which frequency and the level of detail of data exchanged through the interoperable interface of the Generic Adapter must be considered *a priori* by service owners. Special needs in terms of data anonymization, or isolation for the technical deployment of services have also to be considered considering the data protection requirements of each partner.

The Interoperability Framework, particularly the components that are part of the InterConnect cloud may also be deployed in several instances, enabling exchange and logical separation (i.e., instances per pilot may be of interest, per building, etc.).

## 2.1 SAREFIZATION PROCESS

The understanding of realizing the need to make data interactions semantically interoperable and the impact of sharing that data is deeply connected with the SAREFization process of the service itself. The SAREFization process is briefly described in Figure 6.



**FIGURE 6 - SAREFIZATION PROCESS**

The SAREFization process steps are detailed as:

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;



#### 4. Technical integration with the Generic Adapter;

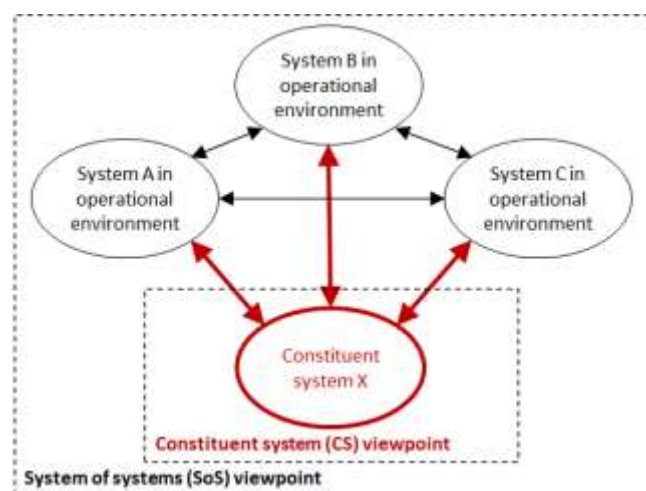
During execution of steps 1 and 2, special focus should be provided to address semantic data modelling, particularly the decision of data to be fed through the interoperable interfaces and their characterization as well as potential privacy sensitivity and level of protection that data requires. Moreover, step number 4, concerning the technical integration should also make sure that Service Specific Adapters taken by services and used as interface towards the Generic Adapter account for the concerns considered when going through step 1 and 2. This should be considered by service owners and teams handling the SAREFization process.

The architecture of the InterConnect Interoperability Framework and its key components is documented in the following InterConnect project deliverables:

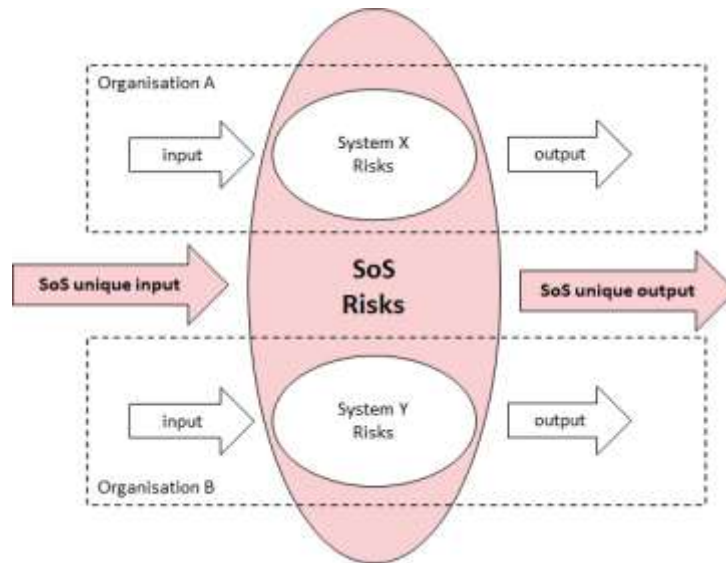
- D2.1 - Secure interoperable IoT smart home/building and smart energy system reference architecture [2].
- D5.1 - Concept, design, and architecture of the interoperable marketplace toolbox [3].
- D5.2 - Data flow management [4].

The InterConnect Interoperability Framework introduces its own set of mechanism for cybersecurity and data protection measures. Each project pilot can be regarded as a semantically interoperable ecosystem with its own set of cybersecurity and data protection (with focus on privacy protection) mechanisms. A project pilot is a system of systems since it comprises digital platforms, services and other data endpoints provided by multiple stakeholders all interconnected with the interoperability framework instantiated for the pilot. The interoperability framework enables establishment of system of system in semantically interoperable manner. Consequently, cybersecurity risks and threats of individual systems (including the interoperability framework) impact overall system of systems/pilot ecosystem. Figure 7 and Figure 8 illustrate the impact from a system of system viewpoint:

- A system X interacts with other systems in an operational environment. Each system is managed and operated independently.
- Two cooperating systems create emerging risks from cybersecurity and data protection perspective.



**FIGURE 7: SYSTEM OF SYSTEM VISION**



**FIGURE 8: SYSTEM OF SYSTEM EMERGING RISK**

The approach selected in InterConnect project is the following:

- Each pilot is the semantically interoperable ecosystem or system of systems provided by multiple independent stakeholders. Pilots comprise one or multiple digital systems (digital platforms and service provisions) maintained by participating stakeholders. These systems bring their own set of cybersecurity and privacy protection capabilities and risks and must be considered when drafting pilot specific plans.
- The interoperability framework stakeholder(s) is a supplier of enablers and services to the pilot ecosystem.
- The pilot negotiates an operating agreement with the interoperability framework supplier in line with the project grant agreement (for the between partner relations and responsibilities) and specific pilot implementation plans (see D1.2 [7]). As a result, the supplier provides information on the interoperability framework security and privacy capability. The agreement follows the project grant agreement and consists of (this approach is also valid for integrators outside of the project consortium):
  - Business agreement in line with the interoperability framework exploitation strategy.
  - Service agreement including cybersecurity, access control and data protection capabilities and requirements.
- Each pilot has its own set of security and privacy protection requirements, plans and threats arising from specific integration challenges required by the conducted use cases.

For each pilot, a Security and Privacy Plan (SPP) is established, allowing for the data security and cybersecurity risks and measures to be expressed. The analysis is established as per the services themselves and assessing the impact of operating the interoperability framework.

The impact from the InterConnect interoperability framework on security and privacy plan of the project pilots (and other integrators outside the consortium) is the following:

- Each pilot SPP must include an agreement with the interoperability framework stakeholder(s).

- Information on the interoperability framework's security and privacy protection capabilities must be provided.

The next sub-sections include an analysis of the security and privacy capability of the interoperability framework. This information is used by the pilots as the basis for implementing their own SPPs and making risks and measurement plans according to their specific needs.

## 2.2 SECURITY AND PRIVACY CAPABILITY OF THE INTERCONNECT INTEROPERABILITY FRAMEWORK

---

The InterConnect Interoperability Framework includes a series of data protection and cybersecurity capabilities, that are built as part of the internal components, namely: the **Service Store**, the **Generic Adapters**, and the **Knowledge Engine** (more information on IF components can be found in D5.1 [3]).

As the key security and identity provider in InterConnect interoperability framework, the Service Store provides means to authenticate and authorize users to engage with the interoperability enablers provided by the framework. The Identity and Authorization Mechanism (IAM) is established by an independent system that is integrated with the Service Store for that sole purpose. This system is an Identify Provider (IDP), where all user accounts are registered, together with the set of roles, granting each user a set of permissions in the interoperable ecosystem. The Service Store acts as the authentication agent, meaning that the IDP system is never directly reached by users' requests, providing the necessary isolation.

The Service Store exposes an API that provides integration mainly with the InterConnect Generic Adapter. This integration provides the means for the described authentication and authorization, but also to other APIs that need to consult the catalogue of interoperable services and their characteristics. All API endpoints are protected by a TLS certificate, signing the channel with SHA-256.

All the operational information of the Service Store is persisted in a relational database system, whose access is configured to be only done by the Service Store backend system, via a non-negotiable access token. The operational database system is isolated with strict access control. Moreover, the operational database holds a hot-standby replica configured with passive replication mechanisms, which provides high-availability over the operational data.

The described components are deployed in a private cloud instance made available by INESC TEC for the purpose of supporting the development stage of the project. Remote access to the machine is only possible via pre-allowed access to a VPN network and via a password-less access with an RSA cryptographic key-pair. Currently, only the key employees from the key stakeholders of the Interoperability Framework have access to such instance. If the system is compromised, backups can be automatically deployed, and compromised components are isolated.

The Service Store backend and frontend systems are available to the WAN via a reverse proxying mechanism that routes the traffic to such instances. Nonetheless, the operational database and the IDP system supporting the Service Store are never available from a WAN connection. The Hot standby replica of the operational database is hosted in a distinct machine, located in the same building, in a different floor.

In terms of privacy protection, when registering in the Service Store as the main identify provider for InterConnect, users are requested to provide a set of personal details, namely their email account from the domain of their organisations, the organisation, the given and

family names. Moreover, a password is requested to support the account creation. The user registration data is validated before being submitted to the system and the password itself is not stored, but rather the result of a deterministic, non-invertible signature. The email account is then verified via a confirmation email sent to that account. After that validation process, the account becomes active. The account creation in the Service Store is bounded by its user agreement in line with the GDPR, requesting consent and strictly explaining the purpose for data collection and processing. Also, in line with the GDPR, accounts and associated data can be requested to be permanently removed at the users' request.

The Service Store acts as the catalogue of all interoperable services. Hence, the service details of all services are available to be consulted by all authorised users. In terms of privacy protection, the service details or their Service Specific Adapters do not hold any sort of operational data, but rather service specific details, such as: service name, service description, integration technology, integration protocol, service category, mapping ontology, mapping ontology version, user that owns the service, creation timestamp, service URL and the platform name.

To enable the semantic data exchange between services (via the InterConnect Generic Adapter), services are required to register their capabilities in semantic terms. That is, each service comprises a set of knowledge interactions, built in the form of RDF triples. This information allows to undoubtedly represent (according to the guiding ontology) the service capabilities and the data comprehending them. That representation is designated as a Graph Pattern. This information is communicated via the InterConnect Generic Adapter and forwarded to the Knowledge Engine component, which stores them as part of its core activity. The exact location of where this information is stored is directly related with the deployment option for this component (check section 2.2.1 for further detail).

While Graph patterns, characterising service capabilities, enable to know what the specific capabilities and data representations are considered in each service, they do not hold operational data of any sort.

The semantic operational data exchange is guided by the InterConnect Generic Adapter. Each interaction is composed by the representing graph pattern (acting as a data model) to which the actual operational data it is bound to. The operational data, in the scope of each knowledge exchange is never persisted by the interoperability framework, being only delivered to the destination Generic Adapter whose interactions semantically match.

The Interoperability Framework allows also to restrict the Services that will receive semantic data exchange in the scope of a knowledge interaction. This allows service owners to authorise or decline the services to receive data, or for the data owners (from the service perspective) to pinpoint the service that will be the sole recipients of their data. This feature, narrows down the number of receivers, thus providing control to the data owner and improving the privacy protection of the framework.

The InterConnect Service Store features the interoperability compliance checks and certification mechanism. The certification solution relies on private permissioned blockchain and smart contracts to store certificates in trusted manner. The blockchain technology utilized for this part of the interoperability framework toolbox is Hyperledger Fabric.

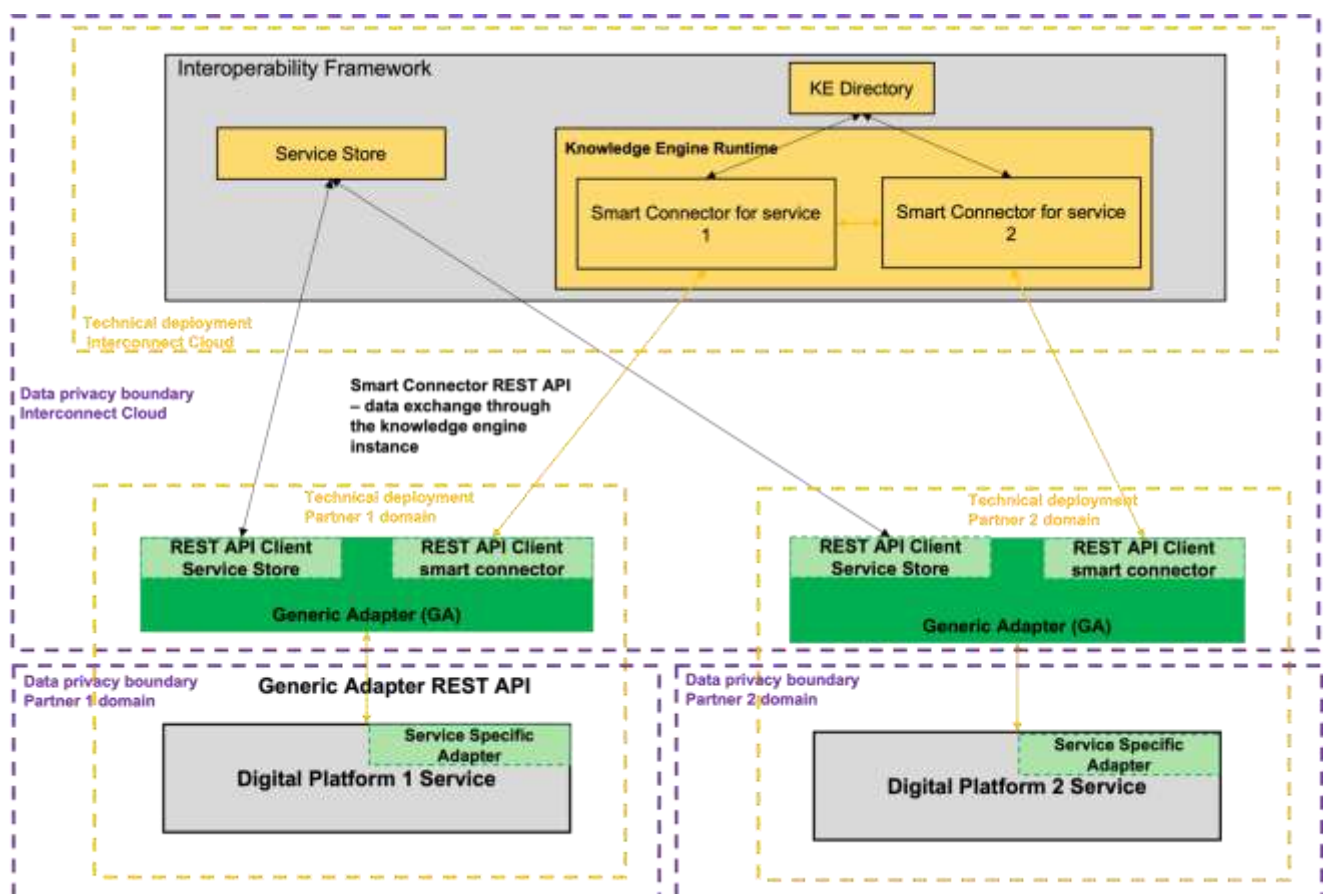
The security and privacy protection features of the P2P marketplace enablers are based on the capabilities of the underlying blockchain technology which is Hyperledger Fabric. The capabilities of the Hyperledger Fabric are described in section 2.2.5.

## 2.2.1 DEPLOYMENT CONSIDERATIONS

The Interoperability Framework was designed and implemented with flexibility of deployment in consideration. This implies that the decisions for deployment of each component should be considered when preparing the pilot's deployment maps, making sure that such decisions are considered in terms of data security and privacy.

This section presents several deployment possibilities and discusses their impacts in terms of technical deployment options and data security and privacy. The main goal is to ensure informed decision taking when addressing pilots' needs.

## 2.2.2 SCENARIO 1: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS AND GENERIC ADAPTERS IN SERVICES DOMAIN



**FIGURE 9 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 1**

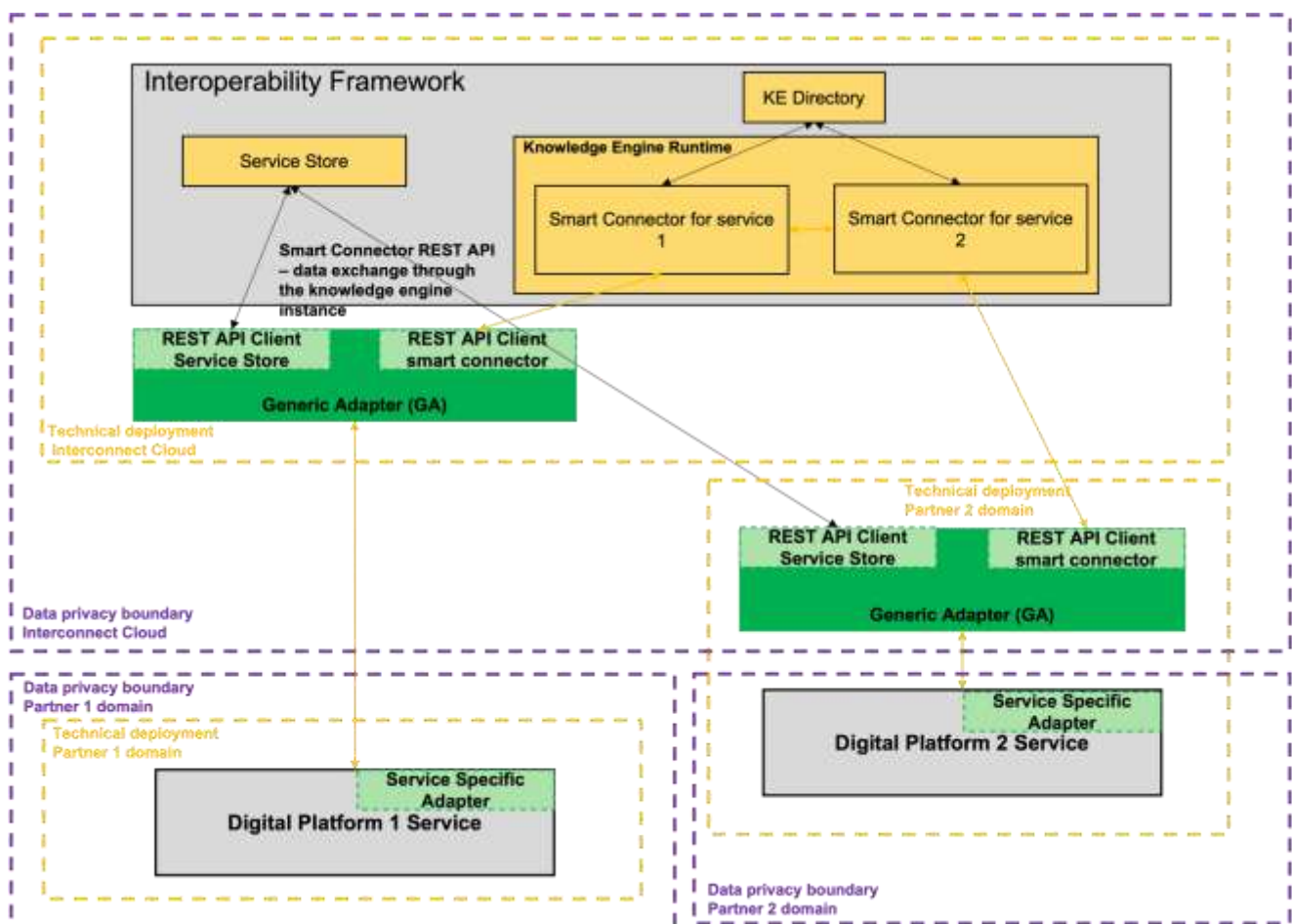
This scenario depicts the concept introduced in Figure 9 as being the deployment option considered as base. It considers the common IF components deployed in the InterConnect Cloud, namely the Service Store and the Knowledge Engine and the SSAs and GAs deployed in the control of Digital Platforms/Service owners. This implies a separation of concerns in terms of the necessary governance of the software components and the data privacy boundary.

Therefore, this scenario configures 3 technical domains and respective data privacy boundaries: the InterConnect cloud, Digital platform 1 and Digital platform 2.



When data is designed to cross any of these borders, service owners must be aware of this decision and accommodate the necessary adjustments. That is, when establishing a relationship with interoperable services from other service providers, in this scenario, data will cross 2 borders: from Digital Platform 1 to the Knowledge Engine in the InterConnect Cloud and from the InterConnect cloud to the destination Service's GA. The Service store will play no active role in the actual data exchange, only feeding the GAs with the set of permissions as recorded by service owners. The knowledge engine will also not persist operation data, maintaining only the Knowledge Interactions and respective graph patterns (SAREFization process step 3).

### 2.2.3 SCENARIO 2: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS AND GENERIC ADAPTERS IN SERVICE AND INTERCONNECT CLOUD DOMAIN

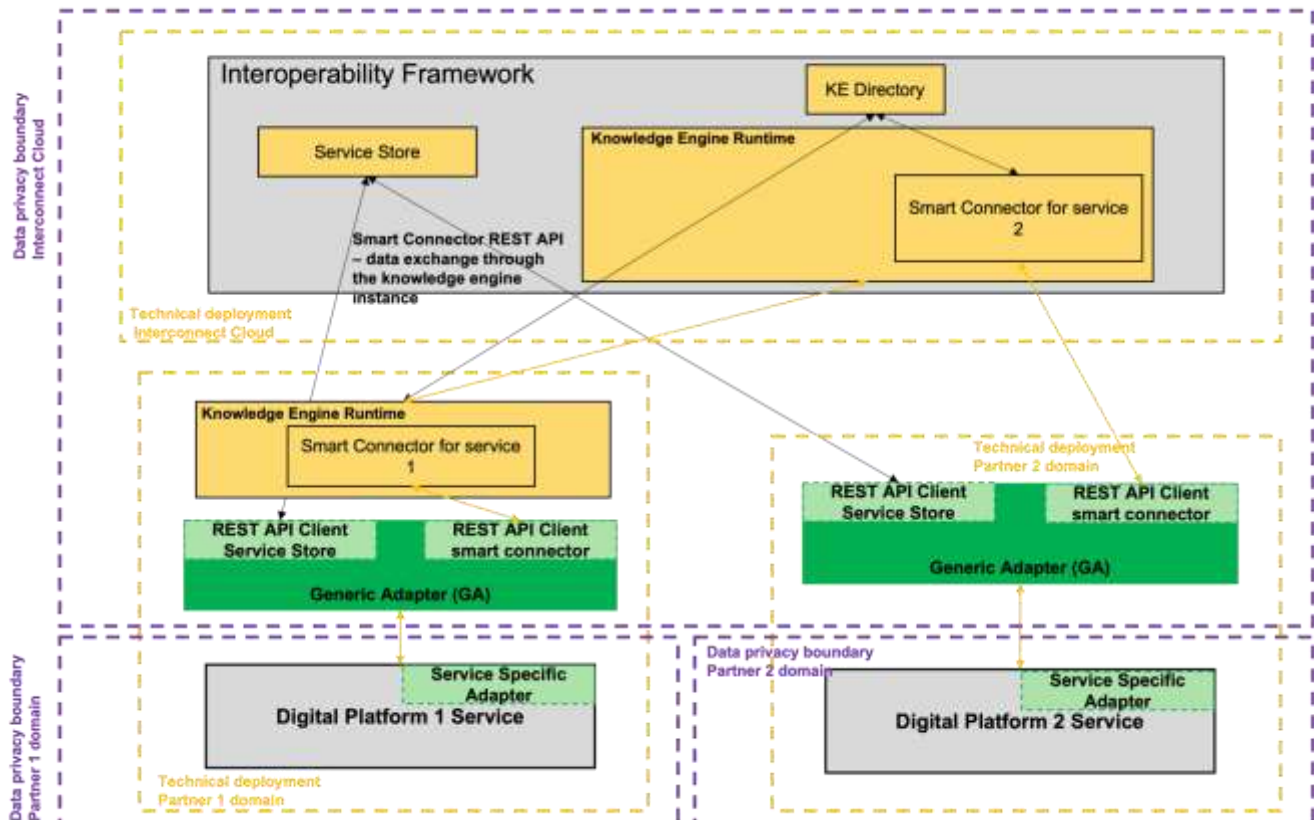


**FIGURE 10 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 2**

This scenario (Figure 10) considers a deployment like the previous one but highlights the possibility that GA's can be deployed in the InterConnect Cloud. In terms of data exchange, this scenario holds the same principle in terms of the data boundaries that are crossed when Digital platform /Service 1 interacts with Digital platform /Service 2 as in the Section 2. The main difference lies in the fact that the technical deployment for the GA in the InterConnect cloud is governed by the InterConnect cloud maintainers but ensuring the data privacy

boundary between Digital platform /Service 1 's SSA and the GA remains for the owner of Digital platform /Service 1 to decide and enforce.

## 2.2.4 SCENARIO 3: COMMON IF COMPONENTS IN INTERCONNECT CLOUD, SERVICE SPECIFIC ADAPTERS, KNOWLEDGE ENGINE INSTANCE AND GENERIC ADAPTERS IN SERVICE DOMAIN



**FIGURE 11 - DEPLOYMENT AND DATA PRIVACY BOUNDARIES (RESPONSIBILITIES) - SCENARIO 3**

This scenario (Figure 11) considers a deployment like the scenario 1 but highlights the possibility that KE can have an active runtime locally deployed in the Digital Platform / Service domain. In terms of data exchange, this scenario holds the same principle in terms of the data boundaries that are crossed when Digital platform /Service 1 interacts with Digital platform /Service 2 as in the Section 2. The main difference lies in the fact that the technical deployment for the KE runtime in the scope of Digital Platform / Service 1 is now within the technical deployment boundary of Digital platform /Service.

Likewise, the persistence of Knowledge Interactions in the KE runtime of Digital Platform / Service 1 is persisted in that domain. Nevertheless, Knowledge Interactions exchange between KE runtimes occurs as part of the expected behaviour of this component.



## 2.2.5 CYBERSECURITY AND PRIVACY PROTECTION IN P2P MARKETPLACES

---

The Interoperability Framework toolbox includes P2P marketplace enablers. These enablers are based on distributed ledger technologies and include: blockchain network configuration, set of smart contract templates to facilitate integration and transaction, order matching engine configurable for specific needs of the marketplace and white-labelled web application as skeleton for further development and integration. The P2P marketplace enablers are provided to the project pilots and other 3rd parties as containers that can be deployed on their own hosting resources. Pilot teams and other integrators become P2P marketplace platform operators responsible for onboarding stakeholders and configuring rules for marketplace operation.

The security and privacy protection capabilities of the InterConnect P2P marketplace enablers and implemented marketplaces (instantiated within the pilots) depend on the capabilities and limitations of the underlying DLT which is Hyperledger Fabric.

Hyperledger Fabric (HF) 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.

Core HF network design components are organizations, channels, smart contracts, and membership service providers (MSPs). In most cases, more organizations will come together to form a channel on which they will interact and where permissions are determined by a set of policies that are agreed to when the channel is originally configured. Moreover, policies can change over time subject to the agreement of the organizations. Smart contracts, or chaincode, are the means through which these interactions occur. MSPs exist to regulate access to resources and identities for all blockchain users.

The security protection measures of HF include the following 4 aspects:

1. Transport Layer Security (TLS) – Fabric supports secure communication between nodes using TLS. This secures, any and all, data transaction interfaces through the HF.
2. Unique Identity – MSP guarantees the legitimacy of the organization and all or its users and applications on the blockchain. Every user/app interacting with the blockchain will have a unique digital certificate that will define its attributes (e.g., location, department) and access parameters. Organizations can use the HF native MSP, Certificate Authority Service, or connect their own MSP/identity provider (e.g., Active Directory). Configurable identity provision management enables pilots to maintain their usual practices or employ the approach inherent from HF.
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. Each P2P

marketplace configuration includes a set of configured policies for each HF channel. This provides flexibility to the integrators to enforce specific access control rules that reflect requirements of their use cases.

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. SDK is typically managed per organization, and the organization is charged with securing access to the SDK layer. All organizations participating in P2P marketplace must utilize proper SDK to manage authorization and access control for the HF channels represented in deployed P2P marketplace.

The privacy protection measures of Hyperledger Fabric include the following 4 aspects:

1. **Multi-channel design** separates the information between different channels. Only organizations belonging to a certain channel can read and write information on that channel. This allows P2P marketplace integrators to fine tune access rights and information flow between participating parties.
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. The organizations belonging to a PDC definition will be able to see the actual data, while others on the same channel will only see the hash of the data. 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 is key feature to grant GDPR compliance of the deployed P2P marketplaces when certain privacy sensitive data (e.g., Smart metering data) must be stored in one of the HF channels.
3. **Controlled Chaincode access** – users/apps can only access the chaincode on the channels their organization is part of. Access is possible through a chosen SDK.
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=FR” can write new data, while users with “viewer” will be able to read data. This sets basis for attribute-based access control to be applied in P2P marketplaces.

All these cybersecurity and privacy protection capabilities of the HF are available to the project pilots and 3rd party integrators who are instantiating the P2P marketplace enablers. They are making final decisions on the security and data protection capabilities that will be employed. There is always a possibility to combine off-chain and blockchain data storage for each P2P marketplace deployment to improve control granularity of the stored data sets. Finally, the applications (e.g., Mobile apps and web apps) and backend processes utilizing the P2P marketplace are to be implemented by the pilot teams and they must introduce additional cybersecurity and data protection measures based on use case requirements and overall sensitivity of the deployed P2P marketplace instance.

## 2.2.6 RELATIONSHIP WITH PILOT SECURITY AND PRIVACY

---

The InterConnect interoperability framework is considered as a subsystem that is integrated in the pilot ecosystem to enable interoperability of all participating systems (digital platforms, services, applications, and devices all provided by different stakeholders). Consequently, the security and privacy risk analysis of the pilot ecosystem must integrate the cybersecurity and data protection capabilities of the InterConnect interoperability framework and its key enablers. To support the security and privacy risks analysis of pilots, this section also identifies higher level security and privacy risks/threats related to the use of the InterConnect interoperability framework. There is a clear boundary between pilot ecosystem and a running instance of the interoperability framework when it comes to data/privacy protection and access control/authorization responsibilities.

When it comes to utilization of the P2P marketplaces within the pilots, the set of marketplace enablers comes with cybersecurity and privacy protection capabilities as described in previous sub-section. P2P marketplace integrators can choose which capabilities to utilize and how to configure them so that complete sets of cybersecurity measures and data/privacy protection requirements are satisfied.

The security and data/privacy protection capabilities of the interoperability framework are one part of the pilot's security and privacy protection plan. Other capabilities and risks must also be considered. The Figure 12 below shows what comprises pilot SPPs and reflects on the system-of-systems methodology behind the pilot deployments. Each pilot SPP includes:

- Security and privacy protection capabilities, risks and threats introduced by each participating legacy digital system (digital platform or a service) as provided by the pilot team members. Pilots might comprise one or more digital systems and their cybersecurity and data protection features are the starting point for building pilot level SPP.
- Security and privacy protection capabilities, risks and threats introduced by the interoperability framework. So, the interoperability framework SPP is integral part of the pilot's SPP if the pilot is utilizing the interoperability framework to establish semantically interoperable ecosystem.
- Each pilot is established around defined use cases and joint business vision of participating stakeholders. This integration and collaboration plan introduces its own set of cybersecurity and privacy protection requirements, risks, and threats. This part of the SPP must be negotiated and prepared by the stakeholders participating in the pilot and is subject to change as the business logic behind the pilot use cases changes and as new stakeholders are added.

The figure below also shows how the pilot SPP is evolving through two stages of workshops organized by the T5.3. It also indicates that the SPP is a living process that evolves and adapts to the changes in pilot organization and goals.

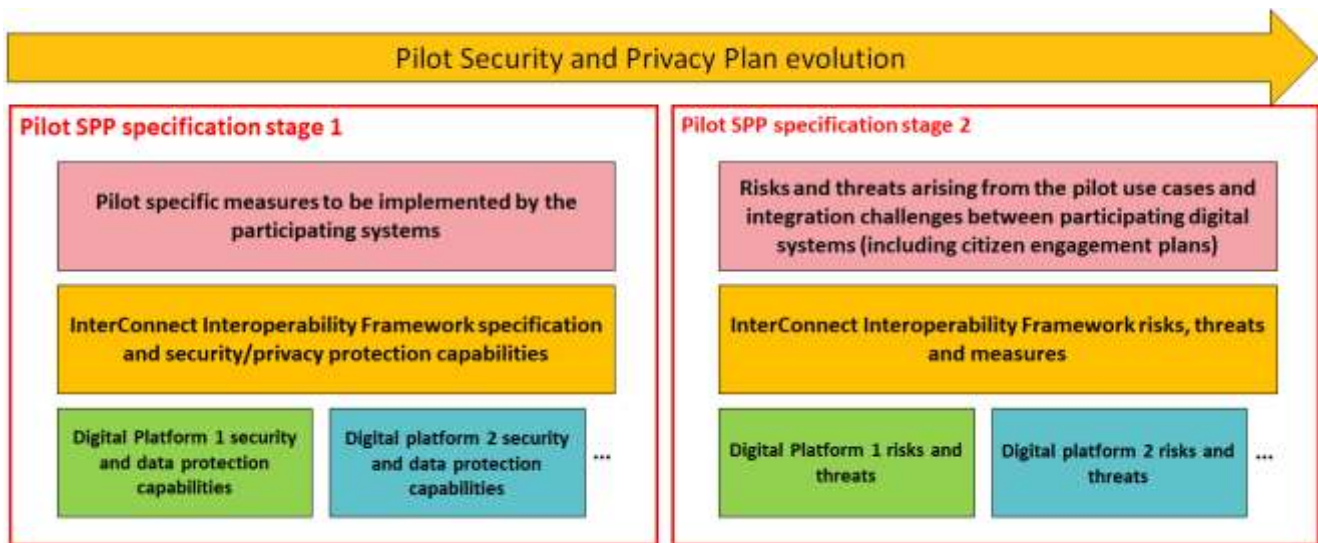


FIGURE 12 - RELATION BETWEEN PILOT SPP AND INTEROPERABILITY FRAMEWORK SPP

## 2.2.7 CHARACTERISATION OF THE INTERCONNECT INTEROPERABILITY FRAMEWORK

Table 3 shows the characteristics of the InterConnect interoperability framework.

Actors	Interoperability framework stakeholder	<ul style="list-style-type: none"> <li>Operates the framework (semantic interoperability layer, service store, P2P marketplace, security framework and access control, admin tools).</li> <li>Provides support to the associated ecosystem (supplying adaptors capabilities or providing support).</li> <li>Can be a set of companies working on the framework development (will be specified in the exploitation strategy).</li> </ul>
	Pilot manager	Operator of an InterConnect pilot or other pilot integrators (outside the consortium).
	User	User of an InterConnect pilot application/service.
	Service provider/owner	An actor that provides a service to another actor (e.g., consent management service, anonymization service)
Use cases	Registering an interoperable service	<p>A service provider uses the InterConnect service store (as part of the interoperability framework) to register an interoperable service. The process goes as follows:</p> <ul style="list-style-type: none"> <li>Service provider registers account (or logins) on the service store and proceeds with service registration or onboarding procedure.</li> <li>Service provider configures generic interoperability adapter in line with its service characteristics.</li> <li>Service provider specifies characteristics of the service.</li> <li>Service provider specifies interface endpoint for the service.</li> <li>Service provider specifies access control rules and authorization levels for the service as part of interoperability framework instance.</li> <li>Compliance test is initiated, and interoperability compliance certificate is provided.</li> <li>Service provider can upload the Docker container for the service. (if required)</li> </ul>
	Onboarding a service	<p>A pilot application uses a service from the service store. This use case involves the following:</p> <ul style="list-style-type: none"> <li>Possibly implementing an interoperability adapter for pilot's own digital platform.</li> <li>Instantiates or utilizes a discovered framework service.</li> <li>Runs compliance tests.</li> <li>Invokes the service.</li> </ul>

	Accessing a service/device from another domain	<p>A pilot application accesses a service from another domain. The semantic interoperability layer is used.</p> <p>This use case involves the following:</p> <ul style="list-style-type: none"> <li>• Uses a semantic interoperability layer to access services from different digital platforms.</li> <li>• Triggers the use of the semantic interoperability layer's orchestration and reasoning.</li> <li>• Involves the use of interoperability adapters on both ends of the communication channel.</li> </ul>
	Access control	<p>A service is enforced by the security framework and access control based on data domains and data boundaries. This use case Involves the following:</p> <ul style="list-style-type: none"> <li>• A service is declared and registered by the service provider.</li> <li>• A remote user from another platform is authorized to access the service by the service provider.</li> <li>• Each access attempt from user involves that security framework verifies access rights and logs the process.</li> </ul>
	Enforcement of usage policies once data has been transmitted	<p>Data transmitted to another domain must comply with provider policies (data sharing agreement). This use case involves the following:</p> <ul style="list-style-type: none"> <li>• A remote user has been granted authorisation to access data provided by a service (e.g., energy consumption profile from a user).</li> <li>• The data comes with specific information concerning user preference.</li> <li>• Remote user creates derived data.</li> <li>• It calls a new service through the interoperability layer which checks that data conforms to the policies.</li> </ul>
	Instantiation of P2P marketplace	<p>Pilot owner can instantiate P2P marketplace enablers for P2P transactions between participating stakeholders:</p> <ul style="list-style-type: none"> <li>• Pilot owner selects proper configuration of Hyperledger Fabric network as immutable ledger.</li> <li>• Pilot owner configures Hyperledger Fabric methods for cybersecurity, access control and data management in line with pilot's requirements.</li> <li>• Pilot owner instantiates set of smart contracts to facilitate P2P marketplace transactions and integration with supporting services and data points.</li> <li>• Pilot owner instantiates web application to support users to utilize P2P marketplace.</li> <li>• Pilot owner invites stakeholders/users to join the P2P marketplace.</li> <li>• Transactions are executed on the instantiated P2P marketplace, recorded in the ledger, and communicated to the enabling services and stakeholders.</li> </ul>
Architecture entities	Service store	Lists all the interoperable services and provides information about service interfaces (for running instances), containers for testing instantiation (sandbox) and discloses services compliance level. Lifecycle orientation with onboarding updates, testing and compliance.
	Security framework and admin tools	<p>Management of access control at service level and supported with instantiated interoperability adapters.</p> <p>Framework administration tools for monitoring status and performance of the framework instances.</p>
	Semantic interoperability layer	<p>Provides cross-domain semantic interoperability, including the following:</p> <ul style="list-style-type: none"> <li>• interoperability discovery, and reasoning;</li> <li>• knowledge directory and connectors;</li> <li>• operational data exchange through unified interface and with data models based on the SAREF ontology.</li> </ul>
	Interoperable service	A service (energy and non-energy) with configured instance of interoperability adapter. Interoperable service can access and utilize all interoperable resources in the ecosystem and in line with predefined access control rights defined by providers of these interoperable endpoints.
	Interoperable device	A device (e.g., smart appliance) running an interoperable service, or directly interfacing with an interoperable service. It exposes device control and status reporting capabilities.
	P2P marketplace enablers	Set of Hyperledger Fabric network configurations, smart contract templates for transactions and integration of data points, white labelled web



		application and interoperability adapter for interaction with wider InterConnect interoperability framework. Instantiated at a pilot level and under the entire control of the pilot ecosystem.
	Application	Applications directly built on top of the semantic interoperability framework instance.
	Legacy applications	Application based on other digital platforms. Requires the implementation and validation of interoperability adapters.

**TABLE 3 - CHARACTERISTICS OF THE INTEROPERABILITY FRAMEWORK**

## 2.2.8 BUSINESS AND CONTRACTUAL CYBERSECURITY CAPABILITIES OF THE INTEROPERABILITY FRAMEWORK

Table 4 shows typical business and contractual cybersecurity capabilities to integrate into the InterConnect interoperability framework.

<b>Interoperability framework cybersecurity and data protection capability</b>	Secure lifecycle of services	Capability to ensure that provided services comply to semantic interoperability protocol through automated testing. All interoperable services should have passed compliance tests before being made discoverable and accessible through instantiated interoperability framework. Through service store and semantic discovery capabilities, each service user will have insight into the achieved interoperability compliance level.
	Secure instantiation of services	Capability to ensure that only services with interoperability compliance certificate can be utilized and instantiated.
	Secure access to services	Capability to ensure that access to services is controlled according to service provider's decisions/business logic and data protection rules. Each interoperable service will be accompanied with a set of access control rules and data handling specification.
	Integrity of interactions based on semantic interoperability framework	Secure exchange of data and metadata through semantic interoperability layer. Note that the orchestration and reasoning capabilities of the semantic interoperability framework are based on distributed knowledge access. Each system component (digital platform, service, application, device) owner will be able to configure how their data endpoint can be accessed and utilized through the semantic interoperability layer.
	Protection of assets used by or accessed through semantic interoperability framework/layer	Protection against tampering of exchanged data and meta data. Protection of semantic interoperability operating assets e.g., knowledge directory and smart connectors which are part of the interoperability adapter. Service store also employs data and asset protection mechanisms for the catalogue of interoperable services and user who have created InterConnect service store account.
	Cybersecurity and data/privacy protection capabilities of P2P marketplace enablers	The P2P marketplace enablers are based on Hyperledger Fabric which introduces a set of measures that are at disposal for security and data protection by the system integrators. Full set of measures is described in section 2.2.5.
	Logging and monitoring performance of interoperability framework instances	All running instances of the interoperability framework will collect performance logs which can be analysed to identify usage and behaviour patterns with high risk of data misuse. Admin tools will be considered for interoperability framework administrators to monitor performance metrics and generate reports.

**TABLE 4 - INTERCONNECT INTEROPERABILITY FRAMEWORK BUSINESS AND CONTRACTUAL CYBERSECURITY CAPABILITIES**

## 2.2.9 TYPICAL SECURITY AND PRIVACY THREATS FOR INTERCONNECT INTEROPERABILITY FRAMEWORK

Table 5 shows the typical security and privacy threats for the InterConnect interoperability framework.

STRIDE threat categories	
Spoofting	<p>Spoofting of service store (malicious service store) – inviting service providers to utilize rogue service store which can misuse their service capabilities.</p> <p>Spoofting of interoperable service (malicious service) – registering an interoperable service which interacts with other openly interoperable services in malicious manner or registering services which mimic other services to interfere with wider decision-making processes.</p> <p>Spoofting of knowledge directory – to interfere with semantic reasoning and discovery operations to achieve malicious benefits.</p>
Tampering	<p>Tampering access rights to bypass access control rules.</p> <p>Tampering data and metadata exchanged throughout semantic interoperability layer to interfere with reasoning and discovery processes.</p> <p>Tampering knowledge directory to interfere with the semantic reasoning and discovery procedures.</p> <p>Tampering configuration of interoperability adapters to impact the way in which interoperable service utilize interoperability framework and other interoperable services.</p>
Repudiation	<p>Repudiation of service access to authorized users.</p> <p>Repudiation of service store or interoperability layer access to authorized and interoperable services.</p>
Information disclosure	<p>Eavesdropping security procedures of the interoperability framework.</p> <p>Eavesdropping service store activity and semantic interoperability layer activity (reasoning and discovery processes).</p> <p>Eavesdropping interoperable service activity to interfere with data exchange or get insight into the exchanged information.</p> <p>Eavesdropping user activities while they utilize interoperable services or applications.</p>
Denial Of Service	<p>Service store denial of service – limiting access to the catalogue of interoperable services or limiting reporting capabilities of running interoperable services. Knowledge directory denial of service – limiting performance of semantic reasoning or discovery processes. Interoperable service denial of service – limit or disable access to running interoperable service to impact its ability to provide information or action necessary for wider system operation.</p>
Elevation of privilege	<p>Incorrect management of user access rights and granting access to limited resources and services to users through manipulation of the semantic interoperability procedures.</p> <p>Bypassing access rights of services which are set based on geographical or regulatory domain constraints through manipulation of the semantic interoperability processes.</p>
LINDDUN threat categories	
Linkability	Associating semantic reasoning and discovery processes and actions with protected data/information and undisclosed identity or business logic of participating stakeholders.
Identifiability	Identify interoperable service/application user based on semantic interoperability processes and decisions.
Non-repudiation	Modifying logged actions and decisions through manipulation of framework monitoring processes.
Detectability	Detecting context of a service user based on semantic interoperability actions (reasoning and discovery).
Disclosure of information	See STRIDE table information disclosure entry.
Unawareness	Unawareness of need for compliance with GDPR or further national regulations for data and privacy detection. Unawareness of semantic interoperability processes and their impact on data protection and service operation if left unconstrained.
Non-compliance	Allowing non-compliant services to impact semantic reasoning and discovery processes.

**TABLE 5 - THREATS FOR INTERCONNECT INTEROPERABILITY FRAMEWORK**



Table 6 shows the identified threats related with the Interoperability Framework with more focus on IF capabilities. Each threat includes an impact assessment with two categories: demo and real. The demo impact assessment refers to the scenario available in the project pilot demonstrations, while the real impact assessment extrapolates the impact in case of a real-world deployment.

Threats related with the Interoperability Framework		
T1	Component	All IF components
	Description	Unauthorized access to the demo system may lead to the inconsistency in the system or its partners, endangering availability, integrity, and confidentiality of the system.
	Impact (demo)	Minor
	Impact (real)	Significant
	Mitigation	Encrypt all inbound and outbound communications via TLS channels
T2	Component	All IF components
	Description	Attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
	Impact (demo)	Minor
	Impact (real)	Significant
	Mitigation	Apply modern cryptography algorithms SSL and maintain them to the latest standard updates.
T3	Component	All IF components via the Service Store
	Description	Unauthorized access to services might compromise system's integrity.
	Impact (demo)	Minor
	Impact (real)	Significant
	Mitigation	Use permission model, based on "Minimal privileges" concept. Separate administrative and non-administrative roles. All callable services should be controlled by proper authorization checks Apply "four-eyed principle": separate Administrator for role assignment.
T4	Component	Service Store
	Description	When JavaScript is printed into HTML page, it could be executed as program code. This may lead to what is called "reflected" or "stored" XSS vulnerability. Unexpected code could be processed on user's machine, making user session stealing possible
	Impact (demo)	Minor
	Impact (real)	Significant
	Mitigation	Ensure application-level proxy with IDS capabilities is considered. Consider keeping sensitive information out of the HTML/DOM, so it could not be modified or stolen. Use "secure" flag when using cookies.
T5	Component	All IF components, particularly Service Store
	Description	Malicious SQL could be put as user input, which results in unexpected SQL statement processed in the database. Malicious SQL query leads to database inconsistency.
	Impact (demo)	Moderate
	Impact (real)	Significant
	Mitigation	Sanitizing input to SQL statements (use "whitelisting" approach), generally don't trust any user input
T6	Component	All IF components
	Description	Malicious File Uploads or Imported files could potentially contain viruses or malware. Malware may endanger system availability, integrity, and confidentiality
	Impact (demo)	Moderate
	Impact (real)	Severe
	Mitigation	Virus checks for all imported files

		Automatic virus scan of all externally transferred to the system documents
T7	Component	All IF components
	Description	Denial of Service (DoS) attack is focused on making resource unavailable for the purpose it was designed.
	Impact (demo)	Minor
	Impact (real)	Severe
	Mitigation	Make sure Anti-DoS proxy is set up, which not only filters incoming traffic by source IP, but also validates it on the application level. Describe recovery plan, which covers procedures needed to quickly restore the system in case of unavailability of some of the components of the server
T8	Component	GA and KE
	Description	Malicious or Misleading content is fed through the GA's and feeds the inferring and/or matching mechanisms to deliver data.
	Impact (demo)	Moderate
	Impact (real)	Severe
	Mitigation	Include validations in the SSAs to verify inbound exchanged data against the Knowledge Interactions expected outcomes before using them in the services business logic. Validate when data bindings are submitted in the scope of knowledge interactions.
T9	Component	P2P marketplace enabler
	Description	Manipulating data written in Hyperledger Fabric blockchain to impact energy and data transactions.
	Impact (demo)	Minor
	Impact (real)	Severe
	Mitigation	The Hyperledger Fabric component of the P2P marketplaces provides different sets of measures for managing access control and data manipulation capabilities for each included channel. Based on the pilot deployment requirements, P2P marketplace enablers are configured to facilitate most secure blockchain network and facilitate all access control rules and data policies required by the pilot. Further updates are possible and must be agreed by all participating stakeholders. Each pilot must define data manipulation policies and trust policies so that any and all blockchain system manipulations are identified and responsible party is excluded from the private permissioned blockchain with overall consensus from all other participants.

**TABLE 6 - THREATS FOR THE INTEROPERABILITY FRAMEWORK**

Table 7 shows the privacy and security threats of the pilot using the InterConnect interoperability.

STRIDE threat categories	
Spoofing	Spoofing one service provider (T_IF1)
Tampering	Tampering knowledge exchange process (T_IF2)
Repudiation	Repudiation of data exchange operation (T_IF3)
Information disclosure	Disclosure of data and metadata by eavesdropping interoperability framework (T_IF4)
Denial Of Service	Preventing the interoperability framework instance to operate (T_IF5)
Elevation of privilege	User of one interoperable service gets access rights to all interoperable services in the pilot (T_IF6)
LINDDUN threat categories	
Linkability	Linking Data and meta data transmitted from two different transactions through semantic interoperability layer (T_IF7)
Identifiability	Identifying user of exchanged data and meta data (T_IF8)
Non-repudiation	N/A
Detectability	N/A
Disclosure of information	Disclosure of consent information and privacy preference information (T_IF9)
Unawareness	N/A

Non-compliance	Consent and privacy preference not handled properly (T_IF10)
----------------	--

**TABLE 7 - THREATS FOR PILOTS USING THE INTERCONNECT INTEROPERABILITY**

## 2.2.10 BREACHES AND IMPACT FOR INTERCONNECT INTEROPERABILITY FRAMEWORK

Table 8 lists the breaches to consider for an InterConnect interoperability framework. Those breaches need to be considered by the pilots.

	Breach	Breach description	Overall impact
<b>B_IF_1</b>	Energy operation disruption	The energy related operations (e.g., grid operation or in-building energy service provision) can be disrupted by manipulating or malfunctioning interoperability framework processes.	Maximum
<b>B_IF_2</b>	Massive cybersecurity breach	A cybersecurity attack prevents operations enabled by the interoperability framework to run.	Significant
<b>B_IF_3</b>	Massive personal data breach	A privacy breach causes a massive breach of business sensitive information of stakeholders or breach of end user personal data.	Significant

**TABLE 8 - BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK**

Table 9 shows how the threats (were they to materialize) can contribute to the identified breaches. The threats have been informally sorted according to an informal assessment of criticality.

		<b>B_IF_1</b>	<b>B_IF_2</b>	<b>B_IF_3</b>
		Energy operation disruption	Massive cybersecurity breach	Massive personal data breach
<b>T_IF1</b>	Spoofing one service provider	X	X	X
<b>T_IF2</b>	Tampering knowledge exchange process	X	X	X
<b>T_IF3</b>	Repudiation of data exchange operation	X	X	X
<b>T_IF4</b>	Disclosure of data and metadata by eavesdropping interoperability framework	X	X	X
<b>T_IF5</b>	Preventing the interoperability framework to operate	X	X	
<b>T_IF6</b>	User of one interoperable service gets access rights to all interoperable services in the pilot	X	X	X
<b>T_IF7</b>	Linking Data and meta data transmitted from two different transactions			X
<b>T_IF8</b>	Identifying user of exchanged data and meta data			X
<b>T_IF9</b>	Disclosure of consent information and privacy preference information			X
<b>T_IF10</b>	Consent and privacy preference not handled properly			X

**TABLE 9 - THREATS THAT CAN CAUSE BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK**

Table 10 provides an impact analysis using the scale proposed in Annex 1.

Impacted perimeter	Impacted item	B_IF_1	B_IF_2	B_IF_3
		Energy operation disruption	Massive cybersecurity breach	Massive personal data breach
Ecosystem	Ecosystem reputation	Significant	Limited	Limited
Organisations	Interoperability framework stakeholder	Maximum	Maximum	Limited
	Pilot manager	Maximum	Significant	Maximum
Citizen	Citizen privacy	-	-	Maximum
		Overall Significant or Maximum	Significant or Maximum	Overall Maximum

**TABLE 10 – IMPACT FROM BREACHES IN INTERCONNECT INTEROPERABILITY FRAMEWORK**

## 2.2.11 MEASURES FOR INTERCONNECT INTEROPERABILITY FRAMEWORK

Table 11 lists measures that have been identified to mitigate the identified threats on the InterConnect interoperability framework (table is based on ISO/IEC 27001 taxonomy of controls). Entries marked N/A are either not relevant or have no identified input. Note that the identified list is indicative. A selection will be made, depending on the needs of pilots.

Category	Sub-categories	Control	Description
Information security policies	Management direction.	Access policies	Access policies are at the service level (interoperable services provided by participating stakeholders).
		Data management policy	Interoperability framework does not store data from end users and managed systems.
Organization of information security	Internal organisation	To be specified in data management plan	
Asset management	Responsibility for assets	Secure storing of service-related metadata and service docker containers	Metadata of interoperable services registered in service store will be secured as well as uploaded service containers – procedure specified for the service store.
Access control	Business requirements for access control	Security and data protection framework	Enforces access to service according to service owner policy and access control rules.
	User access management	Enforce authorised service access	Uses security and data protection framework to validate access to a service and enforce authorization levels specified by service provider.
	System and application access control	Service store web application	Service store access granted only to registered and authorized users.
		Interoperability layer	Interoperability layer access granted only for registered services with interoperability compliance certificate.
Cryptography	Cryptographic controls	Secure exchange	Secure exchange with service store and semantic interoperability layer.
Operation security	Operational procedures and responsibilities	Trustworthy interoperability	Trustworthy exchange capabilities support from services and interoperability framework providers.
	Protection from malware	Service store protection	Secure service store from deployment of malware code.
	Backup	Service store	Data replication for backup purposes of the operational data for the service store.

		Knowledge directories	Wherever appropriate, data replication for backup purposes of the operational data for the knowledge directories
	Logging and monitoring	Logging behaviour of SIL	Logging activity of SIL and identify cybersecurity attack patterns, risks, and threats.
	Control of operational software	Certified services	Services are tested for compliance and receive a certificate necessary for inclusion in the interoperability framework instance.
	Information systems audit considerations	Explain decisions	Provide a log of how the interoperability framework use rules to create outcome.
Communication security	Network security management	Secure running instance of service store and knowledge directory	Rely provider's network security mechanism. Implement additional measures where needed
	Information transfer	Secure transmission	Secure transmission of data, meta data, knowledge between interoperable endpoints.
System acquisition, development, and maintenance.	Security requirements of information system	Security of interoperable services	Each service provider can specify access control and data protection rules for own service.
	Security in development and support processes	Privacy by design	Follow privacy by design in developing interoperability framework and its pilot instances.
		Secure service lifecycle	The development of services follows a lifecycle process where security is integrated
	Test data	Testing operation of interoperable services	Each service provider should prepare test data to test and certify interoperability compliance of a service before inclusion into the interoperability framework instance.
Suppliers' relationships	Information security in supplier relationships	Interoperability framework service level agreement	Provided by interoperability framework stakeholder(s) to adopters/integrators.
	Supplier service delivery management	Interoperability framework service level agreement	Service level agreement indicates how interoperability framework components are delivered and managed independently.
Information security incident management	Management of information security incidents and improvements	Service store and knowledge engine logs	Wherever appropriate, all performance and monitoring logs will be stored in secure manner and used to generate reports for all operational incidents.
Information security aspects of business continuity management	Information security continuity	Assurance of availability	Assurance of service store and semantic interoperability layer availability against DoS
		Monitoring vulnerabilities	Periodic analysis of security and privacy risk, and review of vulnerabilities
	Redundancies	Add redundant capabilities to avoid denial of service	Examples of measures are the following: <ul style="list-style-type: none"> <li>Standby service store.</li> <li>Standby interoperability layer enablers.</li> <li>Standby interoperable services (e.g., multiple running instances or Docker container ready to be deployed on demand).</li> </ul>
Compliance	Compliance with legal and contractual requirements	GDPR and cybersecurity compliance verification	Verification that SIL complies to GDPR regulation and Cybersecurity Act.
	Information security reviews	Compliance of regular services	Verify secure lifecycle of interoperable services.
		Compliance of framework services	Verify secure lifecycle of interoperability framework services and enablers.

**TABLE 11 - MEASURES IN INTERCONNECT INTEROPERABILITY FRAMEWORK**

Table 12 shows how the measures contribute to address the identified threats.

		T_IF1	T_IF2	T_IF3	T_IF4	T_IF5	T_IF6	T_IF7	T_IF8	T_IF9	T_IF10
		Spooing one service provider	Tampering knowledge exchange processes	Repudiation of data exchange operation	Disclosure of data and metadata by eavesdropping interoperability framework	Preventing the interoperability framework to operate	User of one interoperable service gets access rights to all interoperable services in the pilot	Linking Data and meta data transmitted from two different transactions	Identifying user of exchanged data and meta data	Disclosure of consent information and privacy preference information	Consent and privacy preference not handled properly
M_IF1	Data management policy	X		X	X	X	X	X	X	X	
M_IF2	Internal cybersecurity preparedness	X	X	X	X	X	X	X	X	X	X
M_IF3	External cybersecurity preparedness	X	X	X	X	X	X	X	X	X	X
M_IF4	Transparency of access control policies	X	X								X
M_IF5	Requirements for service provider access	X					X				
M_IF6	Privacy preference management										X
M_IF7	De-identification of domain data sets							X	X		
M_IF8	Secure exchange	X	X		X		X	X			
M_IF9	Semantic interoperability of trustworthiness	X	X								
M_IF10	Distributed record of processing							X			
M_IF11	Transparency capabilities	X	X	X	X	X	X	X	X	X	X
M_IF12	Explain reasoning decisions		X								
M_IF13	Secure knowledge creation		X								
M_IF14	Assurance of knowledge published		X								
M_IF15	Secure service lifecycle	X									
M_IF16	Consent and preference management service						X				X
M_IF17	Assurance of availability					X					
M_IF18	Monitoring vulnerabilities	X	X	X	X	X		X	X	X	X
M_IF19	Redundancy to avoid denial of service					X					
M_IF20	GDPR and cybersecurity compliance										X
M_IF21	Compliance of regular services	X						X	X	X	X
M_IF22	Compliance of framework services	X									

**TABLE 12 - RELATIONSHIP BETWEEN MEASURES AND IDENTIFIED THREATS IN THE INTERCONNECT INTEROPERABILITY FRAMEWORK**

## 2.3 INTEROPERABILITY FRAMEWORK SPP

In this subsection we provide SPP from perspective of the InterConnect interoperability framework. Each project pilot (and other integrators of the solutions) should include these SPP components into their overall SPP if they are to instantiate and utilize the interoperability framework. The SPP of the interoperability framework will be further developed as the WP5 progress with implementation and validation of the framework enablers.

1 Security and Privacy Plan Context	
Application Name	InterConnect Interoperability Framework
Summary	The InterConnect interoperability framework is developed by the project to enable semantic interoperability of digital platforms, services and devices allowing them to establish system of systems for realization of the envisioned use cases.
Description	<p>In order to meet the overall semantic interoperability objectives of InterConnect project, as well as requirements of defined use cases, a project pilot is using the interoperability framework, operated by stakeholders of InterConnect (further designated as interoperability framework stakeholders), according to the interoperability framework terms and conditions/service agreement.</p> <p>The InterConnect interoperability framework includes enablers for secure semantic interoperability of digital platforms, services, applications, and devices comprising the pilot. The semantic interoperability provided by the framework enables all these pilot systems to register and discover each other's capabilities, exchange information in unified manner and perform semantic reasoning to infer new knowledge. See D5.1 [3] for more details on the architecture of the interoperability framework and its components and visit the project GitLab to get familiar with the developed framework software components.</p>

2 Governance Management Plan	
Rules and legislation	<p>GDPR for privacy protection.</p> <p>Privacy by design applied to development processes.</p> <p>The interoperability framework is developed in line with the InterConnect project DoA.</p> <p>Interoperability framework T&amp;C agreement – to be specified as part of the MS8 release.</p>
International Standards	SAREF ontology for data modelling.
2.1 Governance Body	
Information Security Manager	Milenko Tosic (VLF), Fabio Coelho (INESC TEC)
Data Protection Officer	Milenko Tosic (VLF)
Other roles	<p>Project partners supporting implementation of interoperability framework in the project pilots:</p> <ul style="list-style-type: none"> <li>• INESC TEC;</li> <li>• VLF;</li> <li>• TNO;</li> <li>• VITO;</li> <li>• Trialog.</li> </ul> <p>WP5 technology “ambassadors” in pilots:</p> <ul style="list-style-type: none"> <li>• Belgian sub-pilots:</li> <li>• VITO, Think E, VUB, OpenMotics, 3E, IMEC, ThermoVault</li> <li>• Dutch pilot: TNO, Hyrde</li> <li>• French pilot: ENGIE, ThermoVault, Inetum, Trialog</li> <li>• German pilot: KEO, EEBUS, IEE, Uni Kassel</li> <li>• Greek pilot: Gridnet, WINGS, Inetum, Cosmote</li> <li>• Italian pilot: PlanetIdea</li> <li>• Portuguese pilot: INESC TEC</li> <li>• Cross pilot: CyberGRID</li> </ul>
2.2 Organisation responsibility	
Entity Name	Interoperability framework stakeholder (INESC TEC, VLF, TNO and other WP5 partners)



	Role	In charge of operating the interoperability framework during the pilot according to the various possible deployment decisions. Also responsible for maintaining and updating the interoperability framework components.
	Address	Institutional addresses of VLF, INESC TEC and TNO can be found on the company websites.
	Contact(s)	Milenko Tosic: <a href="mailto:milenko.tosic@vizlore.com">milenko.tosic@vizlore.com</a> , Fábio André Coelho: <a href="mailto:fabio.a.coelho@inesctec.pt">fabio.a.coelho@inesctec.pt</a>
	Entity Type	Group of organizations
Structure of responsibility		<p>The interoperability framework operator is responsible for maintaining the security and privacy protection of the interoperability framework to the stated level in the interoperability framework agreement.</p> <p>The interoperability framework operator is responsible for the following:</p> <ul style="list-style-type: none"> <li>• Documenting the security and privacy protection capabilities of all framework components and maintaining the documentation as the solution evolves. Documentation is always at disposal to the solution integrators in the official release material (source code, technical documentation, and best practice examples of implementation).</li> <li>• Aligning the interoperability framework data protection processes with the project wide data management plan. This is periodic process performed in each yearly quarter of the framework development process;</li> <li>• Carrying out a security and privacy risk management to ensure that the interoperability framework is at an acceptable level as stated in the terms and conditions/agreement. This risk assessment and management plan will be applied during execution of the project pilots and rely on constant flow of feedback from the pilot ecosystems;</li> <li>• Provision of a statement confirming that the provided system has the right level of protection and that the security and privacy risk analysis is up to date. If and when an identified security and privacy protection risk materializes or a new one is identified, pilot teams will be notified to stop utilization of the interoperability framework until the interoperability framework operators provide solution (software fix).</li> <li>• Monitoring the security and privacy status of the interoperability framework</li> <li>• Discuss in the terms and conditions/agreement with the pilot on actions to be taken in the case of an interoperability framework cybersecurity or privacy breach (service store, p2p marketplace, SIL, access control, administration tools), such as stopping execution of pilot parts and proposed use cases affected by the identified issue until the problem is solved.</li> </ul>
<b>2.3 Rules and procedure</b>		
Meetings		Both the pilot manager and the interoperability framework operator will agree on a list of meetings where the security and privacy status of the interoperability operator will be reported. The interoperability framework stakeholder will organize weekly sync meetings to discuss and present the latest developments and decisions with respect to interoperability framework components including those impacting security and data protection. Each pilot team has at least one representative in the weekly sync calls organized by the interoperability framework operators (project WP5).
Nomination		Each identified task and action point will be assigned to specific organization(s) responsible for its implementation and status reporting. The project GitLab is utilized for submitting support tickets/issues that can be labelled as bug, notification, identified risk/breach, support questions, required/desirable feature, or to-do/planning. Each submitted support ticket is analysed and appropriate action is taken to address it.
Publication of minutes		Status and action points will be published in the Minutes of Meeting (MoM) for each periodic meeting held within WP5/interoperability framework operator group. MoM are uploaded and shared through the project shared drive for documents. When MoM is ready all involved partners are notified and invited to comment and update.
<b>2.4 Continual improvement</b>		
Meetings		<p>Meeting reporting on the security and privacy status will also cover possible improvement to include during the project, or beyond the project (for instance when a measure to be implemented should the interoperability framework be used at a larger scale).</p> <p>Interoperability framework stakeholder organizes weekly sync meetings focused on continuous development and maintenance of the interoperability framework components and instances within project pilots.</p>
Evaluation procedure		<p>Feedback from pilot developers and pilot participants will be reported to the interoperability framework stakeholder. Focus will be put on identified security and privacy protection threats and risks.</p> <p>The project GitLab issues boards are used for submitting tickets indicating required or desired features to be included into the interoperability framework including those related to</p>

	the cybersecurity and privacy protection. Each support ticket is assessed by the framework operator team and action plans on addressing the issue are agreed.
--	---

<b>3 Data Management Plan<sup>6</sup></b>		
Interoperability framework operator is a PII controller and PII processor. InterConnect data management plan is the reference for implementation of the interoperability framework related data management plan.		
<b>3.1 Pilot needs and resources for security and privacy data management</b>		
Ownership of data	Interoperability Framework Stakeholder owns data related to operation of the interoperability framework (logs and statistics); Interoperability framework integrator – in the context of InterConnect project it is a pilot integrating the framework – own all data which represent services, platforms, devices, and end users participating in the pilot.	
PII Controller <sup>7</sup>	Interoperability Framework Stakeholder, Providers of interoperable services and enablers, Operator of local instance of the interoperability framework (e.g., pilot)	
PII Processors <sup>8</sup>	Interoperability Framework Stakeholder, Providers of interoperable services and enablers, Operator of local instance of the interoperability framework.	
PII Principals <sup>9</sup>	Service Store user, Interoperable Service Operator.	
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach	Users registering to the InterConnect service store will be provided with terms and conditions and privacy policy which they need to accept to proceed. These agreements and policies are provided by the interoperability framework stakeholder and checked and confirmed by the project's data protection officer. This end user privacy policy agreement manages the profile and usage of the service store and the semantic interoperability layer components. Privacy policies related to end user data collection and processing by interoperable services participating in the pilots are provided by the service providers and under their direct responsibility. Service providers must disclose impact of participation in instance of the interoperability framework on data collection, transmission and storing.	
Agreement <sup>1</sup>	Organizations	Interoperability framework operator/stakeholder and integrators of the framework.
	Agreement template	Standard service agreement and GDPR compliant privacy policy will be provided.
<b>3.2.2 Data description</b>		
Data 1 – Service store user profile	Dates for collection	Data collected during user registration on the InterConnect service store. Users can be service providers, framework integrators and individual users who would like to browse the catalogue of interoperable services and engage with them.
	Identification of data	Given Name, Surname, Email, Organisation, Cryptographic hash of user chosen password for securing the account.
	Type of data	Textual UTF_8 encoded data.
	Life Cycle	Data is collected via the interoperability framework service store UI or via its programmatic API. Data is validated for type conformity (for instance, user email requires a minimum length and hold the @ character) and store in the IDP (identity provider) system of the service store. User descriptors are also stored in the operational database of the service store for internal reference.
	Data description	Given Name: The given name for the user creating the account. Surname: The Surname for the user creating the account. Email: The email account for the user creating the account to be used at login. Organisation: The User's organisation. Password: Cypher text to be considered for assembling the cryptographic hash of user chosen password.
Data 2 – Service	Dates for collection	Data is collected during registration/onboarding of interoperable services to be include in the Service Store.

<sup>6</sup> The pilot may have two or more applications. The data management plan should be repeated for each application.

<sup>7</sup> ISO/IEC TR 27550 definition: Privacy stakeholder that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

<sup>8</sup> ISO/IEC TR 27550 definition: Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

<sup>9</sup> ISO/IEC TR 27550 definition: Natural person to whom the personally identifiable information (PII) relates

	Identification of data	Service Name, Service Platform Name, Ontology, Ontology version, Service Type, Responsible user, Responsible User Organisation, Service Description, Service Organisation logo or image, Service API description, service URL.
	Type of data	Textual UTF_8 encoded data, openAPI service description in JSON or similar format.
	Life Cycle	Data is collected via the interoperability framework service store UI or via its programmatic API. Data is validated for type conformity, processed and stored in the operational database for the service store. Data related to the openAPI description is processed for service certification and validation purposes.
	Data description	Service Name: The name for the service. Service Platform Name: The platform in which this service is included. Ontology: The primary ontology considered in this service. Ontology version: The version for the primary ontology considered in this service. Service Type: The category for this service. Responsible user: The user that created this service entry. Responsible User Organisation: The organisation from which the responsible user belongs. Service Description: A textual description of the service purpose. Service Organisation logo or image: The logo or image that the responsible user's organisation uses. Service API description: the openAPI description that characterizes the capabilities for that given service. Service URL: the domain name where the is service is available.
Data3 – Semantic interoperability data stored in SIL	Dates for collection	When interoperable service is onboarded onto the service store, service provider utilizes the generic adapter or the service store interface to register knowledge interactions representing the service capabilities and requirements in the SIL.
	Identification of data	Graph patterns presenting knowledge interactions that interoperable service offers. Graph patterns are knowledge interaction representations utilized in the InterConnect SIL based on Knowledge Engine.
	Type of data	JSON, Graph patterns represented as RDF triples.
	Life Cycle	Data is provided during interoperable service configuration and integration with the InterConnect SIL. Data can be retrieved, updated, and deleted on service provider request. Data is stored in the knowledge engine and used for semantic discovery and reasoning. Knowledge Engine can be deployed globally on the level of the project or instantiated and maintained by each pilot as well as individual platform operators. Different deployment decisions result in different jurisdictions over the stored knowledge interactions data.
	Data description	More information on knowledge interactions and their data representation can be found in the project GitLab under the Knowledge Engine repository and its documentation.
3.2.3		Data exchange
Data flow		<p>The data exchange process for the Data-1 and Data-2 descriptors incurs in the following flow: Data is collected either i) via the data form at the service store frontend application considering the user browser application or ii) via the client implementation of the service store API instantiated by the user.</p> <p>For case i) data travels from the user's browser application and the service store backend system via a tunnel cryptographically enabled by the service store frontend server TLS certificate.</p> <p>For case ii), data travels from the service store API client instantiated by the user via a tunnel cryptographically enabled by the service store TLS certificate.</p> <p>For Data-3 flow is: providers of interoperable service provide JSON representations of graph patterns representing all knowledge interactions of their services in two ways: i) service store interface is used to upload graph pattern representation of the knowledge interactions. Service store backend system utilizes the SIL REST API to register knowledge interactions in the Knowledge Engine. Service store can use the same REST API to retrieve information about all registered knowledge interactions and present them to the user; ii) through generic adapter REST API service provider can register and manage knowledge interactions. The generic adapter utilizes the REST API of the knowledge Engine to register and manage knowledge interactions of the service which the generic adapter represents.</p>
Data access control chart		Data access control is established via token-based access control mechanisms as established by OAuth2.0 (only for the Service Store IDP, and not exposing the interface). For details check D5.2 Fig. 14 and Fig.15. Bearer Token is used to secure and authorize usage of the REST API methods.
3.2.4		Data access monitoring
Data access verification procedure		The IDP system and the login mechanisms provide monitoring and control system of system access via the System administrators actor for the interoperability framework. Data access rules can be configured on the side of the backend system of the IDP/service store and through the generic adapter configuration.

3.2.5	Data registry
Registry of agreements	During user registration (all types/classes of users) the terms and conditions and privacy policy is provided to be read and accepted to finish the registration process. During service onboarding process each service provider is asked to read and accept terms and conditions and privacy policy. A record of the accepted agreements and policies is registered for auditability purposes.
Registry of data sets	The service store backend system provides registry of user accounts and service metadata information. The SIL also provides registry of all knowledge interactions and service metadata used by the semantic discovery and reasoning mechanisms. Knowledge interaction graph patterns are stored in smart connectors representing each interoperable service and in knowledge directory storing all registered knowledge interactions and used for the purpose of semantic orchestration.
Registry of citizen consents	As these tools will be publicly available, anyone will be able to register. The service store entity accounts for privacy concerns (provide and manage privacy policies) while keeping trace information from web browser cookies.

4	Risk Management Plan
4.1	Pilot needs and resources for security and privacy risk management
Context for privacy analysis	An initial list of privacy threats for the interoperability framework and associated measures is derived in the scope of the WP5. The threat and risk analysis and mitigation plan for the interoperability framework will be integrated with the SPP of each pilot instantiating the framework components. Privacy sensitive data are handled in the service store (part of user identity) as described in the previous table. The interoperability framework does not store any other privacy sensitive data from end users of the interoperable services and applications. Each project pilot will instantiate interoperability layer and a set of interoperable services. Each service provider and corresponding digital platform operator is responsible to protect privacy of the collected and processed information. Privacy sensitivity of the knowledge interaction data of a specific service depends on the nature of the service and what interactions it exposes. Services which deal directly with end user devices and preferences (e.g., HEMS) have knowledge interactions which might be used to infer knowledge about privacy sensitive information even if not directly provided. It is up to provider of the interoperable service to make sure to completely anonymize all knowledge interaction representations so that direct inference of private information is not possible. The SIL stores all knowledge interactions in secured storage and provides access to the information based on the configured access control rules issued by the service provider.
Context for security analysis	List of security threats for the interoperability framework and its instantiation in the project pilots is being identified in the scope of the WP5 and documented at the start of section 2 of this document. All APIs and databases which are part of the interoperability framework are secured with best practice techniques. Complete process and implementation decisions will be documented in the D5.4 scheduled for September 2021. Pilot operators and adopters of the interoperability framework are responsible for securing access to their services and applications as well as for securing data stores under their jurisdiction. The threat analysis of the interoperability framework will be a continuous process as the framework is tested in the pilots, we envision that more threats and risks are identified.
Context for the project	Each project pilot will utilize the InterConnect interoperability framework. All the risks and threats identified for the interoperability framework will be disseminated and handled with all project pilots.
4.2	Risk management process
4.2.1	Security
Methodology	The interoperability framework security protection and risk mitigation process follow the methodology from D2.1 [2] and D5.1 [3]. Updated methodology will be prepared as part of the future deliverable document D5.4 and be published as a stand-alone document to be maintained throughout the project course. Project pilots will use information provided by interoperability framework stakeholder on its security risk/threat analysis. Workshops on implementation of the interoperability framework within pilots are organized periodically and include discussion and workshop on impact of the interoperability framework risk/threat assessment onto pilot instantiations. Pilot operators will provide feedback on applicability of the threat/risk mitigation actions and mechanisms which will result in updated processes.
Schedule	August - September 2021 – workshops with pilot teams on plans for utilization of the interoperability framework. Details about framework integration and its impacts on the security and privacy protection of the pilot processes.

	<p>September 2021 – methodology documented as part of the MS8 release.</p> <p>September 2021 – end of the project – continuous support and updates of the methodology based on pilot's feedback.</p> <p>After the project – exploitation and support strategy to be defined.</p>
<b>Template</b>	The same template used by the project pilots is used for the interoperability framework stakeholder.
<b>4.2.2</b>	Privacy
<b>Methodology</b>	<p>The interoperability framework privacy protection and related risk/threat mitigation process follow the methodology from D2.1 [2] and D5.1 [3]. Updated methodology will be provided as part of the future deliverable document D5.4 and be published as a stand-alone document to be maintained throughout the project course.</p> <p>Project pilots will use information provided by interoperability framework stakeholder on its privacy and data protection risk/threat analysis. Following the system of systems concept, each pilot needs to assess risks of the existing digital platform for privacy beaches and then assess how the risks/threats identified for the interoperability framework impact overall privacy protection requirements.</p> <p>Workshops on implementation of the interoperability framework within pilots are organized periodically and include discussion and workshops on impact of the interoperability framework risk/threat assessment onto pilot instantiations. Pilot operators will provide feedback on applicability of the threat/risk mitigation actions and mechanisms which will result in updated processes.</p>
<b>Schedule</b>	<p>August-September 2021 – workshops with pilot teams on plans for utilization of the interoperability framework. Details about framework integration and its impacts on the security and privacy protection of the pilot processes.</p> <p>September 2021 – methodology documented as part of the MS8 release.</p> <p>September 2021 – end of the project – continuous support and updates of the methodology based on pilot's feedback.</p> <p>After the project – exploitation and support strategy to be defined.</p>
<b>Template</b>	The same template used by the project pilots will be used for the interoperability framework stakeholder.

<b>5</b>	<b>Engineering Management Plan</b>
Pilot needs and resources for security and privacy engineering	<p>The interoperability framework provides the following security and privacy protection functionalities:</p> <ul style="list-style-type: none"> <li>• Service store mechanisms for user registration and authorization to access interoperable services.</li> <li>• All services will need to pass interoperability compliance tests to be included into the semantic interoperability processes and listed in the service store. Each update to the service will require new compliance test to be performed. Certificates of interoperability compliance will be written in project wide private permissioned blockchain.</li> <li>• Configurable access control module for generic adapters which service providers can adapt to their business and data protection logic.</li> <li>• Identity provider system as part of the service store can interface with identity provider systems of the services and digital platform owners.</li> <li>• Registry of knowledge interactions can be managed by service providers so that registered interactions can be deleted and updated.</li> <li>• Different SIL deployment options are provided to the pilots so they can decide to use project level SIL or instantiate SIL on the level of the pilot or individual stakeholders. This allows pilot stakeholders to take full control over the SIL and registry of knowledge interactions and data routing through the SIL.</li> <li>• Service store database is secured.</li> <li>• Docker containers of interoperable services will be secured within service store.</li> <li>• Semantic interoperability processes are secured and temper resilient.</li> <li>• Integration with OAuth2.0 mechanism so that multiple identity validators can be integrated into the framework instances. Performance logs and reports will be provided and used to identify new risks and threats.</li> </ul>



Engineering process	<p>Engineering tasks within WP5 have distinct responsibilities for each interoperability framework component. This engineering process is agreed by 26 participating partners working together on specification, implementation, and integration of the interoperability framework components.</p> <p>One development task focuses on implementing service store, semantic interoperability framework and access control and authorization framework.</p> <p>One task is dedicated to security and privacy protection plan of the interoperability framework and the pilots.</p> <p>One task is dedicated to implementation and instantiation of P2P marketplace enablers based on distributed ledger technologies.</p> <p>Finally, there is task which will provide continuous updates and maintenance of the running instances of the interoperability framework.</p>
Schedule	<p>Starting from April 2021 the first pilot team members received early access to the interoperability framework enablers to perform proof of concept integrations with their digital platforms and services and start building the processes behind pilot use cases. These early experiments and integration efforts are conducted in controlled environments without engagement of end users. Data used for experiments and validation are anonymized or emulated to avoid privacy breaches and mitigate risks for the early technology provisions. Feedback from the early adopters/integrators was translated into updates of the interoperability framework and its security and privacy plan.</p> <p>The first complete and validated implementation of the interoperability framework will be provided to the project pilots by September 2021.</p> <p>From September 2021 until project end the interoperability framework stakeholder(s) will provide continuous support and updates to the interoperability framework with specific process for addressing security and privacy protection risks and identified issues.</p>

6	Citizen Management Plan
Pilot needs and resources for engagement	<p>The service store is the main point through which end users can directly engage with the interoperability framework. Service and application providers from the pilots are responsible for providing interfaces for engaging end users included in their use cases.</p> <p>Pilot specific citizen engagement plan is responsibility for each pilot leader team.</p>
Engagement process	<p>Project promotes the capabilities and achievements of the interoperability framework to wider public with focus on solution integrators and developers. Standard project dissemination and communication channels are used here. Several webinars are planned for showcasing interoperability framework capabilities and demonstrating the technology to wider public.</p> <p>Pilot specific citizen engagement plan is responsibility for each pilot leader team.</p>
Schedule	<p>Service store will be publicly accessible starting from September 2021.</p> <p>Example videos and promo material will be provided throughout the course of the project.</p> <p>Pilot specific citizen engagement plan is responsibility for each pilot leader team.</p>

The InterConnect interoperability framework (IF) SPP and all the security and privacy protection capabilities, threats, risks, and measures presented until this point of the deliverable, are supplied to the project pilots as inputs to help them make final decision about additional measures then must apply to secure their semantically interoperable ecosystems.

As previously discussed, each pilot comprises a set of digital systems (digital platforms, services, devices) integrated in semantically interoperable manner with IF instance. Therefore, SPPs and threat/risk/impact/measure analysis of each pilot is based on capabilities and SPP of the IF, capabilities of the underlying digital systems and specific challenges behind the interoperation decisions made between pilot stakeholders.

The following sections (3 to 10) provide characterization and analysis results of security and privacy protection capabilities, threats, risks, and measures for each project (sub)pilot. The analysis results presented in these pilot sections are derived by the Task 5.3 team based on

the information collected from the pilots through a series of workshops and provided templates (see Annex 1). For each pilot section the following is included into the analysis report:

1. First, a short pilot description and characterization table is provided listing key actors, pilot use cases and architecture elements comprising the pilot ecosystem.
2. Then the Analysis report for security and privacy protection capabilities and risks is provided with the following logic:
  - a. Pilots indicate if they are utilizing interoperability framework. If they are (all but one sub-pilot from Germany), then the security threats, risks, impact, and measures identified and documented for the interoperability framework apply to the pilot ecosystems.
  - b. Security and privacy protection capabilities of the participating digital platforms are presented. This characterization of the digital platform capabilities comes from the WP5 catalogue of digital platforms (see D5.1 [3]).
  - c. Additional security and privacy protection capabilities to the ones of IF are listed.
  - d. Additional threats and risks to the ones identified for IF are listed.
  - e. Additional actionable measures that pilots will take as well as elaboration on how IF measures will be adapted to certain pilots are listed.



### 3. PILOTS IN BELGIUM

The Belgium pilot consists of 8 different sub-pilot implementations led by different partners and deployed in different locations. Each sub-pilot has its own set of use cases and is based on specific digital platforms.

Regarding this particularity, we have split section 3 into 8 subsections, one per each sub-pilot. Each pilot prepared SPP, and following the planning, each pilot has performed a security and privacy risk analysis. The results and report of the conducted risk and threat analysis are shown in the following subsections. The SPP tables of all pilots can be found in the Annexes of this document.

#### 3.1 NANOGRID KOBEGEM (LED BY: THINK-E)

Nanogrid is a small-scale pilot attempting a holistic view of the Energy communities. Pilot characterization is depicted in Table 13. For description of the common actors and architecture components please refer to the section 3.

<b>Actors</b>	Interoperability framework stakeholder, pilot manager, user, and service provider	
<b>Use cases</b>	"Connectionless" maximization of flexibility in Energy Community	This use case describes how to maximize community flexibility without depending on external sources of information. This use case uses local measurements and calculations to offer energy services like peak shaving and increase in self consumption. The intention of the use case is to be the "fallback" option in case of connectivity challenges with energy market or third-party operators.
	Voluntary (non-) participation in Energy Community	This service provides users of a pilot the possibility to connect and disconnect to the energy community. Users of the pilot will have the option to temporarily not participate in the energy and non-energy services of the site.
	Peer to peer exchange between (virtual) Energy Community	This use case describes peer to peer energy trading between multiple (virtually) connected energy communities. Optimization can happen on inter-community level meaning assets from both communities can be used to offer flexibility to each other. This use case will make use of the peer to peer enabling framework provided by the InterConnect project.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Gateway - EMS	One device integrating the interoperability layer and the proprietary protocols to the different devices in the pilot. The device acts as a gateway to a cloud database but also as an EMS system deciding when devices need to be turned on or off.
	Cloud database	Storing time series data from the measurement points in the pilot.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 13 - CHARACTERISATION OF NANOGRID KOBEGEM PILOT**

#### 3.1.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

##### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited, as listed in Table 14. This pilot does not include any of the digital platforms from the WP5 digital platform catalogue.

Capability	Description
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Network authentication	WPA2 encryption of network access
External access only through VPN	Wireguard VPN used to restrict external access to data.
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room)

**TABLE 14 PILOT CYBERSECURITY CAPABILITIES OF THE NANOGRIID KOBEGEM PILOT**

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. It does not identify any additional threats or breaches specific to the pilot.

### Measures for identified threats

Pilot will use the measures provided by the IF analysis.

### Additional actionable measures

More concrete, as it is stated in Table 14, the control within the category “Access control” and “User access management” is used by this pilot with no additional control to be implemented by the pilot side in this category or in others.

This pilot does not provide a citizen engagement plan, this is the reason why the principal capabilities to integrate are more focused on security than on privacy.

The pilot is reinforcing two specific controls:

1. Communication security -> Network communication security management, which from the IF perspective is relying on network provider, but in this case, the pilot is adding measures to this by the means of: a) network firewall protection for the whole pilot, reinforcing the secure network access; b) network authentication based on WPA2 encryption. These measures are implemented in addition to M\_IF8 Secure exchange, which addresses threats of Spoofing, tampering a service, disclosure of data and metadata by eavesdropping, elevation of privilege from one service access to more than one and linking data and metadata from two different transactions.
2. Access control -> user access management, which is provided by the IF, but within the pilot area two additional measures are established: a) VPN access for external access; b) physical access restriction to the hardware that controls the assets (locked room). Both measures try to avoid the maximum risk to lose the control of the system, from being hacked, by restricting the access to the pilot core system.

**SPP of the pilot is provided in Annex 2.1.1.**

## 3.2 CORDIUM HASSELT (LED BY: VITO)

The Cordium pilot is collecting several Personal Data and other data about consumptions. The pilot is characterized in Table 15:

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, End User and Service provider	
<b>Use cases</b>	Community Cost optimization – district & building level	Minimize DHN operating costs by: <ul style="list-style-type: none"> <li>• Efficient operation of the DHN (lowering the temperature)</li> </ul>

		<ul style="list-style-type: none"> <li>Minimize electricity invoice by means of peak shaving, maximizing RES self-consumption and adapting to dynamic tariffs, all within grid constraints set by a (simulated) DSO</li> </ul>
Architecture entities	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	IoT Data capturing platform	Azure based platform to collect all IoT data and to transport commands towards the devices and systems on site.
	BEMS	Building Energy Management System performing the optimization and execution of the strategy at building level
	DEMS	District Energy Management System application performing the optimization and execution of the strategy at district level. Interacting with the building and optional providing flexibility to a flexibility aggregator.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 15 CHARACTERIZATION OF CORDIUM HASSELT PILOT**

### 3.2.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited. In this pilot, there are several management systems that interact in the pilot, apart from the Interoperability framework. The pilot is ensuring one additional cybersecurity capability as shown in Table 16. While Table 17 gives information about security and privacy protection capabilities of the participating digital platforms.

Capabilities	Description
Access restriction (towards employees)	It implies a physical access restriction to the rooms where assets are and to IT systems that manage the pilot.

**TABLE 16 CYBERSECURITY CAPABILITIES OF CORDIUM HASSELT PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
Dynamic Coalition platform (VITO)	Compliant	Controller/ for Cordium and ThorPark deployments	See API (only API)	REST	API Key & TLS/SSL	No	No	Domain based, user group based, user based
BEMS (VITO)	Compliant	Controller	See API (only API)	REST, MQTT	API Key & TLS/SSL	No	No	NA

**TABLE 17 - DIGITAL PLATFORMS PARTICIPATING IN THE CORDIUM HASSELT PILOT**

#### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. there are two threats in addition to the ones identified in the interoperability framework. These additional threats are related to privacy:

- Non-repudiation: Ability for a user or an entity to deny having performed an action that other parties can neither confirm nor contradict.

- Unawareness: Unawareness of GDPR or further national regulations for data and privacy detection.

In the security and privacy analysis, both threats relate to the *Personal Data Breach*. The impact to the different perimeter remains the same as for the interoperability framework analysis.

### **Measures for identified threats**

The pilot is using the following measures from the interoperability framework:

- Access control: all the measures implemented by the IF are being used by the Cordium Hasselt pilot.
- Cryptography: all implemented measures.
- Operation security: Protection from malware. The service store protection from deployment of malware code.
- Communication security: all measures are used by the pilot.
- System acquisition, development, and maintenance: security requirements of information system and test data sub-category. In this last one, measures to prepare test data and certify interoperability compliance are used.

### **Additional actionable measures**

The pilot will implement the following additional measures:

- Information security policies -> specific data management policies (access control, protection, transparency, business agreements).
- Organization of information security -> Internal organisation: System access restriction, by limiting the number of accounts to the minimum.
- Human resource security -> During employment: Internal cybersecurity preparedness (training and preparedness against cybersecurity attacks to pilot ICT system).
- Human resource security -> Termination and change of employment: Revocation of access rights from all relevant accounts granting access to VITO, project and pilot IT systems and databases.
- Asset management -> Responsibility for assets: Definition of asset responsibility.
- Access control: business requirements for access control, user access management, user responsibilities, system and application access control applied to the pilot's stakeholders.
- Cryptography: Ensure de-identification of relevant datasets (unlinkability).
- Physical and environmental security: physical access to IT buildings with electronic key, the IoT data capturing is done in Azure cloud.
- Operation security:
  - Operational procedures and responsibilities: Definition of operational procedures and responsibilities.
  - Protection from malware: applied the malware protection of VITO IT policy.
  - Backup: VITO data backup policy.
  - Logging and monitoring: monitoring service with associated alert management used to monitor operational behaviour.
  - Control of operational software: Code integrity, code repository restrictions, control version and automated testing.
  - Technical vulnerability management: Separation of concern in software and services development, by means of different operation domains, operation and data protection using separate knowledge Engine Run-time (KER) environments (all IC pilot operations are managed by VITO, there is no external partner involved).

- Information systems audit considerations: Traceability mechanisms implemented to trace back actions.
- Communication security: policy network security management and secure transmission (secure exchange of data).
- Information security incident management -> management of information security incidents and improvements: according to VITO policies.
- Compliance:
  - Compliance with legal and contractual requirements: GDPR and cybersecurity compliance (inherent in VITO policy).
  - Information security reviews: Regular IT security audits at company level.

SPP of the pilot is provided in Annex 2.1.2.

### 3.3 THOR PARK GENK (LED BY: VITO)

This pilot is set in office buildings and a parking and offer different services to users. The only personal data collected directly from users is the EV charging information (arrival, charge, departure times) this results in a relaxed citizens engagement plan.

The characterisation of the pilot is depicted in Table 18.

Actors	Interoperability framework stakeholder, Pilot manager, User, Service provider	
Use cases	Community Cost optimization – district & building level	This use case describes the energy management service at Thor park at two levels: <ul style="list-style-type: none"> <li>• The energy management service offered by a BEMS at building level for each associated building in Thor park to minimize the energy invoice at building level by means of peak shaving, maximizing RES self-consumption and adapting to dynamic tariffs.</li> <li>• The energy management service offered by a DEMS to coordinate the energy consumption and production at district level by means of flexibility negotiation, all within grid constraints set by a (simulated) DSO. The DEMS also includes flexibility requests from flexibility aggregators like cyberGRID when defining a coordination strategy.</li> </ul>
Architecture entities	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	IoT Data capturing platform	Azure based platform to collect all IoT data and to transport commands towards the devices and systems on site.
	BEMS	Building Energy Management System performing the optimization and execution of the strategy at building level
	DEMS	District Energy Management System application performing the optimization and execution of the strategy at district level. Interacting with the building and optional providing flexibility to a flexibility aggregator.

TABLE 18 CHARACTERISATION OF THOR PARK GENK PILOT

#### 3.3.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

##### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited as listed in Table 19. The same digital platforms as in Cordium Hasselt pilot participate in this pilot.

Capabilities	Description
Access restriction (towards employees)	It implies a physical access restriction to the rooms where assets are and to IT systems that manage the pilot.

**TABLE 19 CYBERSECURITY CAPABILITIES OF THOR PARK GENK PILOT**

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. The pilot identifies two additional privacy related threats:

- Non-repudiation: Ability for a user or an entity to deny having performed an action that other parties can neither confirm nor contradict.
- Unawareness: Unawareness of GDPR or further national regulations for data and privacy detection.

In the security and privacy analysis, both threats affect to the *Personal Data Breach*. The impact to the different perimeter remains the same as for the interoperability framework analysis.

### Measures for identified threats

This pilot has the same approach for identified threats and measures as the Cordium Hasselt pilot described in the previous section. The additional measures, to the ones identified in the interoperability framework analysis, are also the same as in the Cordium Hasselt pilot. Both pilots are led by VITO and company policies apply to both. The only difference in the plans and measures is the geographic location of the pilots.

**SPP of the pilot can be found in Annex 2.1.3.**

## 3.4 STUDENTS ROOMS TOWER ANTWERP (LED BY: IMEC)

This small-scale pilot is in a university campus building with shared spaces among students and a set of appliances that are used in communal manner. As it is situated in a public building, privacy is not the focus of the pilot, the analysis and measures are more oriented to cover security aspects. Table 20 characterizes the pilot.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	Gamification of use of common appliances	Reduce energy consumption and flatten the energy profile of the building by: <ul style="list-style-type: none"> <li>• Inform the students best time to use electricity (i.e., off-peak hours)</li> <li>• Inform the students of the overall building consumption</li> <li>• Allows the students to use collectively smart appliances and awards them when doing so</li> </ul>
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	DYAMAND	Local framework that offers a middleware solution to the problem of device interoperability
	Cloud database	Storing time series data from the measurement points in the pilot.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 20 CHARACTERISATION OF THE STUDENTS' ROOMS TOWER ANTWERP PILOT**

Apart from the IF, the pilot utilizes the Dyamand framework locally to integrate the devices that will be part of the pilot.



### 3.4.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited as listed in Table 21. While Table 22 gives information about security and privacy protection capabilities of the participating digital platform.

Capability	Description
Confidentiality and Authenticity of data	Secured network protocols
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Logical Access restriction (towards users)	Access to the application is restricted to registered users. Sign up process follows a Two-factor authentication
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room).

**TABLE 21 CYBERSECURITY CAPABILITIES OF THE STUDENT'S ROOMS TOWER ANTWERP PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
<b>DYAMAND (IMEC)</b>	NA/ Middleware relaying data of other compliant entities	NA/ middleware not an entity itself	OIDC	GraphQL / custom	TLS/ SSL/JWT	No	No	Domain based, user group based, user based

**TABLE 22 - DIGITAL PLATFORM PARTICIPATING IN THE STUDENT'S ROOMS TOWER ANTWERP PILOT**

#### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. There are not additional threats or breaches identified by the pilot.

The impact to the different perimeter remains the same as for the interoperability framework analysis, except for the cybersecurity data breach with impact set to minor/limited.

#### Measures for identified threats

The pilot is using the following interoperability framework measures:

- Access control: all the access control subcategories with their measures identified by the interoperability framework.
- Cryptography: For the secure exchange.
- Operation security -> Protection from malware.
- Communication security (network security management, information transfer): All the measures provided by the interoperability framework are used by the pilot.

#### Additional actionable measures

No additional measures are identified for the pilot.

**SPP of the pilot is presented in Annex 2.1.4.**

### 3.5 SMART DISTRICT NIEUWE DOKKEN GENT (LED BY: DUCOOP)

This pilot implements an EMS platform where users can manage the energy consumptions through cooperation and as part of energy community. The pilot is represented in Table 23:

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	Optimal battery management	With overarching goal to increase self-consumption.
	Optimal district heating management	With overarching goal to increase use of renewable sources cost-efficiently.
	Heat demand forecasting	To be able to reach optimal district heating management.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices.
	Gateway device - district level	Connects with assets (battery, heat pump...) and ingests operational data into database.
	Gateway device - individual unit level	Connects with private appliances (lighting, heating, meters...) and ingests data into database.
	Database(s)	Stores data coming from district level assets and individual living units.
	Cloud - EMS	Connects with database (to get operational data), executes control algorithms, and connects with gateway device (to send control actions).
	Cloud - Forecasting application	Connects with database (to get historical operational data and forecasted data) and executes forecasting models. These forecasting applications are offered as services in the InterConnect Service Store.

TABLE 23 CHARACTERISATION OF DE NIEUWE DOKKEN PILOT

#### 3.5.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

##### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited as listed in Table 24. While Table 25 gives information about security and privacy protection capabilities of the participating digital platform.

Capability	Description
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Two-factor authentication	Any access to OpenMotics cloud/hardware can be restricted with 2FA
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room)

TABLE 24 CYBERSECURITY CAPABILITIES OF DE NIEUWE DOKKEN PILOT

Platform name (partner)	Security and privacy protection attributes						
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security
Cloud Platform (OpenMotics)	Compliant	Controller	OAuth	REST	OAuth Token & TLS/SSL	No	No
							User / Role based

TABLE 25 - DIGITAL PLATFORM PARTICIPATING IN DE NIEUWE DOKKEN PILOT

## Threats and breaches identification

This pilot inherits the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens. There are not additional threats identified or breaches, just some specifications in threats already identified by the IF analysis:

- The spoofing is not only affecting a service provider (threat identified by the IF) but also an energy asset or an authorized employee (threats identified by the pilot).
- The tampering, with personal or district-level data.
- Information disclosure: it can be caused by unintended data breach by employees or partner when they grant access to database to third parties without legal basis or permissions to do it.
- Linkability, identifiability and detectability: anonymization might be insufficient measure to avoid identification of data subject.

The pilot splits the data breach into personal data breach and business data breach as a significant breach. Business data breach can inference the control algorithms or disclose business sensitive data of a partner. Usually, these breaches are caused by threats identified in the spoofing, tampering and information disclosure subcategories.

The impact to the different perimeter remains the same as for the Interoperability framework analysis, except for the cybersecurity data breach with impact is set to minor/limited.

## Measures for identified threats

The pilot is using the following interoperability framework measures:

- Access control: all the access control subcategories with their measures identified by IF.
- Cryptography: For the secure exchange.
- Operation security -> Protection from malware.
- Communication security (network security management, information transfer): All the measures provided by the IF are used by the pilot.

## ***Additional actionable measures***

The pilot introduces the following additional measures:

- Organization of information security:
  - Internal organisation: the pilot implements a system access restriction, limiting the number of accounts to the minimum.
  - During employment: Internal cybersecurity preparedness, continuous awareness of the importance of cybersecurity measures to pilot ICT systems.
  - Termination and change of employment: Revocation of access rights when an employee finishes his/her relationship with the partner.
- Asset management:
  - Responsibility for assets: definition of asset responsibility between stakeholders.
- Access control:
  - Business requirements for access control: Access tracking, a list is kept and regularly updated of all the users with access to the pilot system, registering the accesses.
  - User access management: user role management by each pilot stakeholder.
  - User responsibilities: responsibilities linked to user roles, internally done by each partner.
  - System and application access control: access linked to user roles.

- Physical and environmental security:
  - Secure areas: Physical key and registration keys.
- Operation security:
  - Operational procedures and responsibilities: definition of operational procedures.
  - Backup: automated database backups for operational and system configuration data.
  - Logging and monitoring: visualised system parameters with alerts (for system operational data and energy operational data), including warning messages when blanks are not filled in. Logging historical data.
  - Control of operational software: Checks at code deployment (continuous integration/deployment engine) that automatically tests code.
  - Information systems and audit consideration: provide a log of how the energy management system uses rules to create control actions.
- Communication security:
  - Network security management: Firewall for the whole network.
  - Information transfer: Secure transmission over standard secure protocols or password-protected email addresses.
- Compliance: GDPR and cybersecurity compliance.

SPP of the pilot is presented in Annex 2.1.5.

## 3.6 ZELLIK GREEN ENERGY PARK BRUSSELS (LED BY: VUB)

This pilot is in Brussels and implements a Peer-to-Peer energy between prosumers. The pilot is characterized in Table 26.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	Peer to peer exchange between (virtual) Energy Communities	This use case describes peer to peer energy trading between multiple (virtually) connected energy communities. Optimization can happen on inter-community level meaning assets from both communities can be used to offer flexibility to each other. This use case will make use of the peer to peer enabling framework provided by the InterConnect project.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Gateway - EMS	One device integrating the interoperability layer and the proprietary protocols to the different devices in the pilot. The device acts as a gateway to a cloud database but also as an EMS system deciding when devices need to be turned on or off.

TABLE 26 CHARACTERISATION OF THE ZELLIK GREEN ENERGY PARK BRUSSELS PILOT

### 3.6.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

Regarding this scenario, the pilot is more focused on security aspects and does not need to implement many additional measures to the ones already implemented and provided by the Interoperability framework. In this case as in the Nanogrid Kobbegem pilot, the main

cybersecurity capabilities are focused on the network security and access, as it is shown in Table 27. This pilot does not include any of the digital platforms from the WP5 digital catalogue.

Capability	Description
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Network authentication	WPA2 encryption of network access
External access only through VPN	Wireguard VPN used to restrict external access to data.
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room)

**TABLE 27 CYBERSECURITY CAPABILITIES OF ZELLIK GREEN PARK ENERGY PILOT**

### Threats and breaches identification

This pilot inherits the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens. There are no additional threats or breaches identified.

The impact to the different perimeter remains the same as for the IF analysis.

### Measures for identified threats

It will use the measures provided by the IF analysis.

### Additional measures

The pilot has identified and/or implemented one additional measure to the measures already provided by the IF:

- Access control - User access management: Enforcing the authorised service access.

**SPP of the pilot is presented in Annex 2.1.6.**

## 3.7 OUD-HEVERLEE PUBLIC BUILDINGS (LED BY: 3E)

The pilot is set in four public buildings. Data collected comes from public entities and not individual private users. The focus of SPP is on evaluating the security of the pilot system and implementing additional measures to secure the synaptiQ platform that extend the ones provided by the interoperability framework. Table 28 characterizes the pilot.

Actors	Interoperability framework stakeholder, Pilot manager, User, Service provider	
Use cases	maximizing self-consumption	Approaching Zero injection
	maximizing self-sufficiency	Approaching Zero withdrawn
	Minimising the electricity bill	ToU or other tariff scheme in place, self-consumption compensation schemes, demand charge management via peak shaving, feed-in or other injection tariffs consideration, and avoiding curtailments. If there is any limit on the grid exchange, it will be also a term of the cost function as a penalty factor
	Flexible power exchange at PCC	Tackling a commanded power for flexibility provision with varying scope, activation time and duration for additional revenue streams with battery, EVs, and building thermal inertia via coordination with HVAC load controller
	Optimal use of storage system	Energy storage is remunerated for the provision of services while some of these services, however, may accelerate battery ageing and degradation and hence this needs to be properly balanced against associated services remunerations.
Architecture entities	Thermal comfort	In coordination with SQP, DQ optimizes the HVAC energy use considering the building thermal inertia and HVAC device activation maintaining comfort level (Not via the Interoperability framework)

	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Field Automation Gateway device integrated by 3E	Connects with assets and meters to ingest operational data into the SQ database and transfer schedules/commands to the device level 3E is reselling BacBee gateways and Webdyn loggers to customers that do not have a solution for OPC and Modbus data acquisition hardware that can send metrics to SynaptiQ over (S)FTP.
	Gateway/platform of local devices	Connects with 3E's local Gateway device (PV, Battery, HVAC units, EV charging station)
	3E's Platform as a service	Such as communication and data servers
	3E's Infrastructure as a service	Such as secure I/O and Account Manager
	3E's Software as a Service	Such as forecaster, optimizer, co-operator. All SynaptiQ services and data depicted above are hosted in a private cloud at InterXion in Zaventem (BE) for EMEA customers, which is a Tier-3 datacenter.

**TABLE 28 CHARACTERISATION OF THE OUD-HEVERLEE PILOT**

### 3.7.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited, listed in Table 29. While Table 30 gives information about security and privacy protection capabilities of the participating digital platform.

Capabilities	Description
Access management policy	Authentication & permissions SynaptiQ account monitoring and logging
Security and data protection: Digital intrusion	<ul style="list-style-type: none"> <li>External security audits.</li> <li>Datacenter services are managed by external host (Advanced Service Provider, ASP).</li> <li>3E infrastructure automatically bans remote IP addresses after several unsuccessful attempts at service level (web servers, data warehouse, ...).</li> </ul>

**TABLE 29 CYBERSECURITY CAPABILITIES OF THE OUD-HEVERLEE PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
SynaptiQ Power (3E)	Compliant	Controller	No	REST	TLS/SSL	No	No	Domain, user group, user based

**TABLE 30 - DIGITAL PLATFORM PARTICIPATING IN THE OUD-HEVERLEE PILOT**

#### Threats and breaches identification

This pilot inherits the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. There are not additional threats or breaches to be listed.

The impact to the different perimeter remains the same as for the Interoperability framework analysis. But the pilot also considers the Technological provider as an organisation that will be



impacted by the breaches, mostly from a *massive personal data breach*, which will be of maximum impact. There will be major implications for the technical provider in searching the source of the leak and solve it in the shortest time to minimize the damage.

### Measures for identified threats

The pilot will use the measures provided by the IF analysis.

### Additional actionable measures

The pilot has identified and/or implemented additional measure to the measures already provided by the Interoperability framework:

- Information security policies:
  - Management direction: data management policy which covers the general data aspects implemented:
    - Only authorized personnel have credentials for remote login to the SynaptiQ infrastructure systems using nominative VPN access certificates.
    - A password policy is in place on account managers & authorized personnel.
    - 3E is currently in the process of implementing Single Sign On functionality for the SynaptiQ service.
    - Penetration testing with an external security firm.
    - Predefined user roles.
- Operation security - Logging and monitoring:
  - All user identification and authentication events are logged, and all logs are available to 3E Support Desk team during the complete SynaptiQ contract period.
  - Logging and authorisation methods for controlling components are however dependent on the control method that is implemented.
  - Distributed record of processing, it registers the historical logging with specific data.
- Information security aspects of business continuity management:
  - Information security continuity:
    - Assurance of availability: an external service is auditing security and testing penetration in the system. BGP Scrubbing serving against Denial of Service. Firewall at the Check point.
    - Monitoring vulnerabilities: Vulnerability Scan: Through Qualys is performed by ASP the vulnerability scan that can be offered to customers infrastructure.
  - Redundancies:
    - Redundancy to avoid denial of service: specific services implemented to avoid DDoS.

**SPP of the pilot is presented in Annex 2.1.7.**

## 3.8 MECHELEN (LED BY: THERMOVault)

This pilot is set in a residential building of 27 apartments, where energy consumption and forecasted household data are collected for the purpose of the use cases. Pilot characterization is shown in Table 31.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider, Flexibility service provider ThermoVault
---------------	--

<b>Use cases</b>	HLUC 1: Peak shaving and self-consumption by optimizing household boilers at community and household level in Genk LEC	Control flexible thermal loads to adapt to new tariff conditions where self-consumption and peak shaving are necessary to reduce LEC-members electricity cost. This includes demand response to increase community-level self-consumption, reduce peak consumption penalties and increase individual-level energy efficiency.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Customer premises	<ul style="list-style-type: none"> <li>• Water heater controller</li> <li>• Space heater controller</li> <li>• White goods</li> <li>• Heat pumps</li> <li>• EMS</li> </ul>
	Application	Applications directly built on top of the semantic interoperability framework instance.

TABLE 31 CHARACTERIZATION OF MECHELEN PILOT

### 3.8.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is not providing any additional capabilities in addition to the ones inherited. Table 32 gives information about security and privacy protection capabilities of the participating digital platform.

Platform name	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
ThermoVault platform	Compliant	Controller	See API (only API)	REST	API Key / JWT	No	No	Role user based

TABLE 32 - DIGITAL PLATFORM PARTICIAPTING IN THE MECHELEN PILOT

#### Threats and breaches identification

The pilot has not identified more threats or breaches than the ones already identified in the IF analysis.

#### Measures for identified threats

It will use all the measures provided by the IF analysis.

#### Additional actionable measures

There is no more specific or additional measure, from this pilot. The actions to be implemented right now are the Internal organisation for the data management plan, the user management access policy, and the protection against DoS by assuring the availability of the system.

**SPP of the pilot is presented in Annex 2.1.7.**

## 4. GREEK PILOT

The Greek presents 9 different use cases focused on energy saving and flexibility services. Users are an important part of the pilot and there are specific use cases to engage them. Pilot characterization is depicted in Table 33.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	Energy Monitoring & Management	Use cases described in “D1.3 System use cases for smart buildings and grids”. For brief information, please see Annex 2.2.
	Home Comfort	
	Flexibility Provision	
	Data Analytics Services	
	Security Services	
	Increase CO2 savings and become eco-friendly	
	User Engagement	
	Unified User Interface Application	
	Appliances Energy Efficiency	
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Backend Services	Cloud services responsible for collecting and distributing data from smart meters and sensors of the participating households
	Devices/Appliances	Various devices to be used – see SPP.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 33 CHARACTERISATION OF THE GREEK PILOT**

### 4.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring certain specific capabilities in addition to the ones inherited as listed in Table 34. While Table 35 gives information about security and privacy protection capabilities of the participating digital platforms.

Capability	Description
Example: Unlinking capability concerning metering dataset Confidentiality, Integrity, Availability Unlinkability, Transparency, Intervenability	Secure hash of PDL (Point de Livraison – Point of delivery)
Anonymization of metering dataset	Personal details are stripped from metering datasets and households are referred with an ID.

**TABLE 34 CYBERSECURITY CAPABILITIES OF GREEK PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
LeonR&Do (COSMOTE)	Compliant	NA/Testbed	HTTP Basic auth for UI SSH Keys auth + VPN	REST / MQTT	TLS/SSL	No	No	Role based access control
Gfi Semantic IoT Platform (Inetum)	Compliant	Controller	HTTP Basic auth for UI oAuth token for API	REST/MQTT	oAuth Token & TLS/SSL	No	No	Per user/role based
HomeGrid (GRIDNET)	Compliant	Controller	JWT	REST/MQTT	TLS/SSL & JWT	No	No	Role based access control
ARTEMIS (WINGS)	Compliant	Processor	OAuth	REST, Kafka Broker, STOMP	TLS/SSL	No	No	Per user/role based

TABLE 35 - DIGITAL PLATFORMS PARTICIPATING IN THE GREEK PILOT

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen. It does not identify any additional threat or breach specific to the pilot.

### Measures for identified threats

It will use most of the measures provided by the IF analysis, except 2 of them (Information security policies -> management direction -> Data management policy, the internal organisation from information security and the Backup measures).

In total, 14 measures are taken by the pilot, already described in the IF analysis.

### Additional actionable measures

In the category of *Human resource security*, the pilot is adding in the measure of internal cybersecurity preparedness during employment. It will implement trainings and preparedness against cybersecurity attacks to pilot ICT system, when and where it is appropriate.

**SPP of the pilot is presented in Annex 2.2.**

## 5. DUTCH PILOT

The Dutch pilot is led by Volkerwessels, and it is focused on Smart buildings to save energy and optimize sustainability. The pilot is depicted in actors, use cases and architecture entities in the Table 36.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	High level use case 'lower the energy costs'	For more information and detail on the use cases description, see D1.3 and Annex 2.3.
	High level use case 'reduce grid peak load'	
	High level use case 'optimize use of RES (renewable energy sources)'	
	Pilot use case 'building management system (sensors and devices)'	
	Pilot use case 'energy management system (devices)'	
	Pilot use case 'smart meter readings'	
	Pilot use case 'EVs and charge lounge'	
	Pilot use case 'battery'	
	Pilot use case 'PV cells'	
	Pilot use case 'get user data and feedback'	
	Pilot use case 'building and home control'	
	Pilot use case 'getting flexible tariffs from energy provider'	
	Pilot use case 'getting grid tariffs'	
	Pilot use case 'forecasting energy, building and EVs'	
	Pilot use case 'send schedule and control energy devices (building, EVs, storage)'	
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Ecko platform	Details provided in SPP.
	Home automation platform	Details provided in SPP.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 36 CHARACTERISATION OF THE DUTCH PILOT**

### 5.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is ensuring one specific capability in addition to the ones inherited, listed below. While Table 38 gives information about security and privacy protection capabilities of the participating digital platforms.

Capabilities	Description
Example: Unlinking capability concerning metering dataset Confidentiality, Integrity, Availability Unlinkability, Transparency, Intervenability	Secure hash of PDL (Point de Livraison – Point of delivery)

**TABLE 37 CYBERSECURITY ADDITIONAL CAPABILITIES OF THE DUTCH PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
ReFlex (TNO)	Compliant	NA/ not managing personal data	HTTP Basic auth for UI	Multiple	Depends on API type	Yes	No	Role based access control
dEF-Pi (distributed Energy Flexibility Platform & Interface) (TNO)	NA/ support framework no data collection	NA/ support framework no data collection	HTTP Basic auth for UI	Multiple	Depends on API type	Yes	No	Data is strictly separated per user
Ekco IoT Platform (Hyrde)	Compliant	Controller	HTTP Basic auth for UI	REST / MQTT	API Key / JWT	Yes	No	Role based access control
Ekco API Marketplace and IoT micropayment platform (Hyrde)	Compliant	Controller	HTTP Basic auth for UI	REST / MQTT	API Key / JWT	Yes	No	Role based access control

**TABLE 38 - DIGITAL PLATFORMS PARTICIPATING IN THE DUTCH PILOT**

In this case, a crucial capability to avoid and reduce risk of many threats is to secure the Point of delivery.

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizen.

### Additional threats identified

In this pilot, there have been detected several possibilities that can, specifically, happen in the system and they could be encompassed in threats already identified by the IF:

- Elevation of privilege:
  - Unauthorized access of actors or from user's devices due to a lost, steal.
  - Unauthorized access to different networks in the pilot.
  - Unauthorized physical access to assets of the pilot.

An additional threat identified by the pilot is:

Unawareness: People working on the solution and parts of the platform are not trained properly. Privacy and privacy engineering can be compromised.

### Additional breach identified

The pilot inherits the 3 breaches from the IF but has identified *A cybersecurity breach in the pilot systems* - Ekco and home automation platforms are not operational or malfunctioning.

The impact of the breach in the system affects:

- Organisations (pilot manager and IF): significant.
- Ecosystem: significant.
- Citizen privacy: limited.

Overall impact remains significant because it limits a part or the total system for the users. If the home automation is not working, they cannot access to any other services.



**Measures for identified threats**

The pilot will use the measures inherited from IF, all of them. But in some of them, the pilot is planning to implement additional measures.

***Additional actionable measures***

In most of the categories that are taken by the pilot from the IF, it is expected to add any additional measure to reinforce the security and privacy:

- Human resource security:
  - During the employment (Internal & external cybersecurity preparedness):
    - The pilot considers organizing awareness meetings with the employees in charge.
    - The pilot considers organizing and prepare materials to be communicated through InterConnect channels.
- Asset management: It is expected to implement additional measures to define the responsibility of assets and the information classification.

**SPP of the pilot is in Annex 2.3.**

## 6. FRENCH PILOT

The French pilot is focused on energy flexibility with two main objectives:

- Maximize the local self-consumption of renewable energy.
- Minimize the cost of consumption.

The pilot is briefly described in the Table 39.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
	Trialog (tech. transf.)	EMS system manager.
	Flex manager (TV)	As energy and flexibility manager, our steering relies on: <ul style="list-style-type: none"> <li>• Leveraging data to forecast the thermal heating demands and available flexibility</li> <li>• Provide energy- and cost-efficient steering on appliances level, considering (time-varying) electricity prices, thermal losses, and household tariff incentives (e.g., self-consumption of local PV power).</li> <li>• Operate a Virtual Power Plant, providing value on the day-ahead, balancing, capacity and ancillary services market.</li> </ul>
	Flex manager (Engie)	The flexibility manager: <ul style="list-style-type: none"> <li>• gets the data it needs to forecast the flexibility</li> <li>• needs real time update to adapt its forecast</li> <li>• activates flexibility in the pool according to the requested flexibility</li> <li>• gets real time feedback from portfolio to adapt the flexibility dispatch</li> <li>• The customer can disable the flexibility if required.</li> </ul>
<b>Use cases</b>	Maximize use of RES	The main goal is to Manage the different customer uses by maximizing renewable energy consumption via smart meter consumption and production data. This service synchronize consumption with RES production at local level. Moreover, this service uses a local storage in the house based on a recycle EV battery. The customer stores the energy produced by his PV in his absence, and he use this energy when he needs it.
	Dynamic tariff	The goal is to offer dynamic tariff that allows users to benefit from lower electricity tariff by acting on their usage to reduce their costs and know better their usage and impact including service management. Dynamic information is used from supplier's offers to adapt the energy consumption to the tariff on-going to reduce bill and carbon footprint.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices.
	Customer premises	<ul style="list-style-type: none"> <li>• EV charger</li> <li>• EMSs service provider (local)</li> <li>• Water heater controller</li> <li>• Space heater controller</li> <li>• T-EMS front-end</li> <li>• White goods</li> <li>• Heatpumps</li> <li>• PV</li> <li>• Linky</li> <li>• ERL of the Linky</li> </ul>
	Application	Applications directly built on top of the semantic interoperability framework instance. <ul style="list-style-type: none"> <li>• T-EMS back end</li> <li>• Manufacturer back end</li> <li>• Metering data platform</li> <li>• EMS service provider</li> <li>• Flex manager</li> <li>• Smart orchestrator</li> </ul>

TABLE 39 CHARACTERISATION OF THE FRENCH PILOT

## 6.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

### Pilot is using the IF

The pilot is using the interoperability framework and it is ensuring two specific capabilities in addition to the ones inherited as listed in Table 40. While Table 40 gives information about security and privacy protection capabilities of the participating digital platforms.

Capabilities	Description
Example: Unlinking capability concerning metering dataset Confidentiality, Integrity, Availability Unlinkability, Transparency, Intervenability	Secure hash of PDL (Point de Livraison – Point of delivery)
Protect against network attacks	IPS

**TABLE 40 CYBERSECURITY CAPABILITIES OF THE FRENCH PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
<b>Tiko platform (Engie/Tiko)</b>	Compliant	Processor	via mobile SMS	REST, THRIFT	TLS encryption VPN	No	No	Per user/ role based
<b>Gfi Semantic IoT Platform (Inetum)</b>	Compliant	Controller	Keycloak (openID, SAML, OAuth)	Kafka, Rest	TLS/SSL	Yes	No	Per user/ role based
<b>EFLEX (ENEDIS)</b>	Compliant	NA/ depends on use case	SAML, OAuth	HTTPS/REST	TLS/SSL	YES	YES	Per user/ role based
<b>Reasoning engine/SLOR (Trialog)</b>	NA/ Works with Linky already anonymized data	NA/ performs ontology mapping of anonymized data	No	REST web services	No	No	Yes	Access control with ontology
<b>ThermoVault platform</b>	Compliant	Controller	See API (only API)	REST	API Key / JWT	No	No	Role based, user based

**TABLE 41 - DIGITAL PLATFORMS PARTICIPATING IN THE FRENCH PILOT**

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens.

#### **Additional threats identified**

No additional threats to the ones from the IF analysis are identified.

#### **Additional breach identified**

The pilot inherits the 3 breaches from the IF and has not identified a new one. In this pilot, they have identified the partners that will be affected and responsible to deal with each breach.

- Breach\_IF\_2 Cybersecurity breach (back-end data)

- (Dynamic tariff data leak) – Engie and Thermovault.
- Trialog – (Linking data and meta data from different transactions).
- Breach\_IF\_3 Personal data breach:
  - Engie (customer data leak).
  - Trialog (Disclosure of consent information and privacy preference information).

The impact of the breaches in the system affects a bit differently and the pilot has split the citizen impact between citizen privacy and customer comfort:

- Organisations
  - IF: All breaches maximum impact.
  - Energy supplier (Engie): All breaches maximum impact.
  - DSO: All breaches maximum impact.
  - Control system service provider (Engie, Trialog, TV, SO): All breaches maximum impact.
  - Pilot manager: B\_IF\_1 and B\_IF\_3 maximum impact, for the B\_IF\_2 the impact is limited.
- Citizen:
  - Comfort: Maximum for Breach 1 and Breach 2.
  - Privacy: Significant for Breach 1 and maximum for breach 3.

Overall impact augments to maximum for B\_IF3 and B\_IF1 but significant for the B\_IF2.

### **Measures for identified threats**

The pilot will use the measures inherited from IF, all of them. There have been identified some actions for the full deployment of the pilot and they are specified in the SPP. It is planned to carry out DPIA in different stages of the pilot. This is the continuous risk management practice.

### ***Additional actionable measures***

There are no additional measures identified by the pilot.

**SPP of the pilot is presented in Annex 2.4.**

## 7. PORTUGUESE PILOT

This pilot is led by EDP and is focused on enabling flexibility in private and commercial buildings.

The pilot is characterized in Table 42.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
<b>Use cases</b>	HLUC 1 Monitoring Energy Consumption	For more detailed information, see Annex 2.5 and D1.3.
	HLUC 2 Subscription of Services for Domestic Energy Management	
	HLUC 3 Data Sharing via Consumer Enabled Preferences	
	HLUC 5 DSO Data Sharing for Consumer & Market	
	HLUC 7 Flexibility Aggregation in Commercial Buildings	
	HLUC 8 Convenient EV Charging	
	HLUC 9 Enabling P2P flexibility sharing within renewable energy community via Blockchain enablers for SAREF services	
	HLUC 10 Flexibility management for Distribution Grid Support	
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	DSO Interface (E-Redes)	Digital platform providing DSO related data and relevant tools (observability, flexibility, metering data, API management) for the pilot.
	SENSINOV	Sensinov's hypervisor provides a single, centralized interface for monitoring and controlling multi-vendor IoT ecosystems. Sensinov's Building Operating System (BOS) centralizes heterogeneous data from existing Building Management Systems (BMS) or devices (HVAC, lighting, alarms, energy meters and IoT sensors) for monitoring, controlling, alerting, and automating building management.
	ThermoVault	ThermoVault flexibility service provision platform includes the energy management system and the control IoT box for retrofitting and smartifying thermal residential loads and activate their flexibility when possible while keeping end-user comfort. Flexibility services include congestion management, voltage control and energy efficiency among other services.
	Cybergrid	Cross-border pilot manager
	INESC (HEMS)	Cloud-based Home Energy Management System (HEMS) providing remote control and monitoring of the users appliances. It manages the user's consumption and optimizes it for economic saving or the use of renewable energy sources.
	Schneider Electric Portugal	Digital platform for commercial buildings.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 42 CHARACTERIZATION OF PORTUGUESE PILOT**

## 7.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

### Pilot is using the IF

The pilot is using the interoperability framework and introduces the following additional capabilities as listed in Table 43. While Table 44 gives information about security and privacy protection capabilities of the participating digital platforms.

Capabilities	Description
Secure protocols	Secure hash of PDL (Point de Livraison – Point of Delivery) Secure protocols should always be used regardless of used channel (between application systems, tools, databases, and devices)
Data segmentation	For the pilot, a new database will be created, segregated from the operational database that will store only the relevant data for pilot demonstration (minimization of data)
User Access Control	Every user will have to be registered and their permissions will be given according to their role on the pilot (minimization of access/permissions) and access and actions will be
Resource monitoring	The resources used by the pilot will be monitored to ensure their correct performance.
Architecture	Logical separation of the different functions of the application, according to its criticality and level of exposure, in accordance with the Cybersecurity Reference Architecture.
Data Management	All related data usage will comply with GDPR requirements, from the beginning (privacy by design)

**TABLE 43 CYBERSECURITY CAPABILITIES OF THE PORTUGUESE PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
HEMS (INESC TEC)	Compliant	Data Processor	OAuth + X.509 cert	REST	TLS/SSL	No	No	Role based access control
Grid and Market Hub Platform (INESCT TEC)	Compliant by design	Data Processor	OAuth + X.509 cert	REST	Path allowance X.509 attributes	Yes	No	Role based access control
Sensinov platform (SENSI)	Compliant	Controller and Processor	JWT	REST	TLS/SSL	No	No	Role based access control
EcoStruxure Building Operation (SEP)	NA/Building level solution no data exchange on Internet	NA/Building level solution no data exchange over Internet	SSH	REST / SOAP /MQTT	TLS/SSL	Yes	No	Domain based, user group based, user based
ThermoVault	Compliant	Controller	See API (only API)	REST	API Key / JWT	No	No	Role based, user based

**TABLE 44 - DIGITAL PLATFORMS PARTICIPATING IN THE PORTUGUESE PILOT**

As the Dutch and French pilot, a crucial capability to avoid and reduce risk of many threats is to secure the Point of delivery.



**Threats and breaches identification**

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens.

***Additional threats identified***

In this pilot, there are not additional threats identified.

***Additional breach identified***

The pilot inherits the 3 breaches from the IF and has not identified a new one. The impacts remain the same for the system.

**Measures for identified threats**

The pilot will use the measures inherited from IF.

***Additional actionable measures***

The additional measures to implement are:

- Information security policies: to manage direction, the service owners only make meaningful and necessary data via the interoperable interfaces.
- System acquisition, development, and maintenance -> security in development and support processes: Secure knowledge creation, to push only meaningful data via the interoperable interfaces.
- Information security aspects of business -> Redundancies: This will be use during the pilot period.
- Compliance -> Compliance with legal and contractual requirements: GDPR and cybersecurity compliance to be done by establishing rules for each privacy boundary by each service stakeholder.

**SPP of the pilot is presented in Annex 2.5.**

## 8. ITALIAN PILOT

The Italian pilot is focused on helping users with enhanced monitoring and control smart devices in homes. The pilot characterization is depicted in Table 45

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, service provider	
	Prosumer	It is intended in a broader view as an active player working with the aggregator (virtual energy producers)
	Balance Service Provider	An actor that provides a service to promote grid stability. This role is not yet defined by the National Regulation but there is an expectation that it will be.
	Aggregator	2 different aggregators: Energy (dynamic tariffs); Flexibility
<b>Use cases</b>	PUC1 - Provide consent to data transfer	For more detailed information, see Annex 2.6.
	PUC2 -Enable flexibility programme	
	PUC3 - exchange of aggregated flexibility data	
	PUC4 - Time of use tariffs	
	PUC5 - Awareness and notification	
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Application	Applications directly built on top of the semantic interoperability framework instance.
	Application (Planet app)	Provides connection between user and pilot services (e.g., send to the energy provider the current start-time for a smart appliance).
	Application (Whirlpool app)	Enable the first connection between Whirlpool smart appliances and the cloud
	Service (Flexibility)	Send a flexibility request to the energy service and monitor the users' response.
	Service (Energy)	React to a flexibility request setting up a new start-time for all the smart appliances connected
	Hardware (Smart appliance)	Once connected to the manufacturer's cloud can be remotely managed by the Planet app (e.g., setting a new start-time for the washing cycle of a washing machine)

**TABLE 45 CHARACTERIZATION OF THE ITALIAN PILOT**

### 8.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and introduces additional capabilities as shown in Table 46. While Table 47 gives information about security and privacy protection capabilities of the participating digital platform.

Capabilities	Description
Secure lifecycle of services	Capability to ensure that provided services comply to semantic interoperability protocol through automated testing. All interoperable services should have passed compliance tests before being made discoverable and accessible through instantiated

	interoperability framework. Through service store and semantic discovery capabilities, each service user will have insight into the achieved interoperability compliance level.
Secure instantiation of services	Capability to ensure that only services with interoperability compliance certificate can be utilized and instantiated.
Secure access to services	Capability to ensure that access to services is controlled according to service provider's decisions/business logic and data protection rules. Each interoperable service will be accompanied with a set of access control rules and data handling specification.
Integrity of interactions based on semantic interoperability framework	Secure exchange of data and metadata through semantic interoperability layer. Note that the orchestration and reasoning capabilities of the semantic interoperability framework are based on distributed knowledge access. Each system component (digital platform, service, application, device) owner will be able to configure how their data endpoint can be accessed and utilized through the semantic interoperability layer.
Protection of assets used by or accessed through semantic interoperability framework/layer	Protection against tampering of exchanged data and meta data. Protection of semantic interoperability operating assets e.g., knowledge directory and smart connectors which are part of the interoperability adapter. Service store also employs data and asset protection mechanisms for the catalogue of interoperable services and user who have created InterConnect service store account.
Logging and monitoring performance of interoperability framework instances	All running instances of the interoperability framework will collect performance logs which can be analysed to identify usage and behaviour patterns with high risk of data misuse. Admin tools will be considered for interoperability framework administrators to monitor performance metrics and generate reports.

**TABLE 46 CYBERSECURITY CAPABILITIES OF THE ITALIAN PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
Planet App (Planet Idea)	Compliant	Controller	OAuth/ JWT	REST web services	TLS/ SSL/ JWT	No	No	Per user/ role based

**TABLE 47 - DIGITAL PLATFORM PARTICIPATING IN THE ITALIAN PILOT**

## Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens.

### **Additional threats identified**

There are not additional threats identified.

### **Additional breach identified**

The pilot inherits the 3 breaches from the IF and has not identified a new one. The impacts remain the same for the system.

### **Measures for identified threats**

The pilot will use the measures inherited from IF.

### **Additional actionable measures**

The additional measures to implement are:

- Information security policy: the pilot will draw up a list of policies to be followed across the partners.

- Organization of information security -> internal organisation: it will align the Human Resources with the previous ones. (Documents are ready for the user security access management and standard operative procedure).
- Asset management:
  - Termination and change of employment: onboarding and outboarding project employee's policy as a crucial part of the access management.
  - Responsibility for assets: Data governance and IT policies will implement the responsible and responsibilities for the assets and its access.
  - Information classification: same as responsibility for assets.
- Access control: rules and policies for access management and responsibilities for users are set up and for the control of the system and applications (at any access point of the systems).
- Cryptography: For all data storage, all PII to be removed or encrypted, also for the business-critical data that will be encrypted. The secure exchange is ensured with a 128-bit encrypted SSL or equivalent.
- Physical and environmental security:
  - Protection from malware and backup: it is also described in the documents for the organization of information security policies and standards.
  - Logging and monitoring: In data exchange agreement includes a distributed record processing which allows one to have a global view of all the processing and its compliance with policies. Logging will be secure and timestamped.
  - Control of operational software: integration of transparency management operations.
- Communication security: Network security management is implemented in the documents for standard operative procedure.
- System acquisition, development, and maintenance: Test data, for this it must have data sharing contracts.
- Information security incident management: It is described in a document the procedures to follow to manage the incidents.

**SPP of the pilot is presented in Annex 2.6.**

## 9. CROSS-BORDER INTEROPERABILITY PILOT

This pilot is not located in a specific country or building, it is an overarching demonstration. It is a cross-border pilot that tries to demonstrate the interoperability advantages through the digital platforms in different countries. The pilot is depicted in Table 48.

<b>Actors</b>	Interoperability framework stakeholder	
	Pilot manager	cyberGRID administrator
	User	Flexibility providers owners – usually business entities
	Service provider	Partners from other pilots
<b>Use cases</b>	Cross-border interoperability	Flex services are offered to a market player, in this case a cyberGRID flexibility management platform, who aggregate flexibility from various flex providers and offer it to (simulated) ancillary market - TSO, to demonstrate cross-border interoperability.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Cross-border pilot architecture	The cyberGRID demonstration will operation within the bounds of the interoperability framework established by InterConnect, whilst also deploying its own architecture for connecting to each pilot. cyberGRID will develop Service specific adapter connecting the cyberGRID platform and the InterConnect framework utilising Generic adapter and the Knowledge engine – InterConnect building blocks to exchange data between the cyberGRID platform and the flex providers.
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 48 CHARACTERISATION OF CROSS-BORDER PILOT**

### 9.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

#### Pilot is using the IF

The pilot is using the interoperability framework and is introducing two new capabilities as listed in Table 49. While Table 50 gives information about security and privacy protection capabilities of the participating digital platform.

Capabilities	Description
The secure communication between the cyberGRID platform and the flex providers	Usually, the VPN technology is used when exchanging data between the flex provider and the cyberGRID FMP – Flexibility management platform to ensure the level of security.
Hashing the operation data	Hashing of data that are not relevant for the operation, such as the POD number, account data.

**TABLE 49 CYBERSECURITY CAPABILITIES OF THE CROSS-BORDER PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
cyberNOC (cyberGRID)	No - business users only	NA/ business users only	OAuth/ OpenIdConnect	Multiple	Api key	Yes	No	Per user/ role based

**TABLE 50 - DIGITAL PALTFORM OF THE CROSS-PILOT SCENARIO**

#### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches and their impact in the ecosystem, organisation, and citizens.

***Additional threats identified***

There are not additional threats identified.

***Additional breach identified***

The pilot inherits the 3 breaches from the IF and has not identified a new one. The impacts remain the same for the system.

**Measures for identified threats**

The pilot will use the measures inherited from IF.

***Additional actionable measures***

The pilot has not identified any additional measures to implement apart from the ones inherited from the IF.

**SPP of the pilot is presented in Annex 2.7.**



## 10.GERMAN PILOTS

The German pilot has a commercial (Hamburg) and residential (Norderstedt) installation. This section is divided per location to provide a clearer explanation.

### 10.1 NORDERSTEDT LOCATION

This pilot is in the city of Norderstedt in residential area. It uses an EMS (Energy Management system) to aggregate energy demands and offers, manage flexibilities and grid commands.

Together with Stadtwerke Norderstedt, the residential part of the German pilot includes key partners who are not part of the InterConnect project with limited freedom to test new technologies. In this case the adoption of the IF will be limited to SAREF compliant communication with the white good devices via cloud platform and the communication between local EMS and backend EMS from DSO.

The pilot characterization is depicted in Table 51.

<b>Actors</b>	Pilot manager, User, Service provider	
	Grid-X local EMS with EMS Cloud as local EMS provider	With the grid-X EMS solution the local intelligent devices will be managed and the WG devices over Cloud
	Stadtwerke-Norderstedt backend solution (MeterPan/IVU)	The backend EMS management provide tariff information and use demand forecast and measurement information for grid stabilisation service
	Stadtwerke-Norderstedt as energy service provider	SWNOR receives measurement information for bill creation based on the tariff definition
	WG manufacture cloud	The Wight good devices will be connected for the flexibility service directly with the EMS cloud.
<b>Use cases</b>	Variable Tariff Calculation	This service uses grid load predictions (from the DSO), off-shore-wind generation predictions (from the TSO) and spot prices (from the energy exchange) to calculate variable grid fees. Furthermore, the service calculates variable tariffs based on the energy delivery prices (e.g., spot prices) and the given taxes/levies for each customer in addition to the variable grid fees.
	Grid Flexibility Protection Service	This service uses information from forecast schedules and real time measurements in combination with grid topology to estimate current and upcoming grid states. For the state estimation, an ANN-approach is utilized. Based on current and predicted grid states and calculations, possible active power grid flexibilities will be computed within this service.
<b>Architecture entities</b>	Customer premises	<ul style="list-style-type: none"> <li>Local EMS with EMS Cloud</li> <li>EV Charger</li> <li>Smart Meter Gateway</li> <li>Added Value Module</li> <li>HVAC system</li> <li>PV inverter</li> <li>Battery inverter</li> <li>White goods devices connected via WG cloud</li> </ul>
	Application	<ul style="list-style-type: none"> <li>Meterplan backend EMS module</li> <li>Local EMS application for all EEBUS appliances</li> <li>Customer application from EMS service</li> <li>Administration application from EMS service</li> <li>Administration application from backend EMS module</li> </ul>
	Application	Applications directly built on top of the semantic interoperability framework instance.

TABLE 51 CHARACTERISATION OF THE NORDERSTEDT PILOT

## 10.1.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

### Pilot is not using the IF

The Norderstedt pilot will focus on the secure connection between DSO and the local energy management with the appliances from the house and will not use the interoperable framework. The pilot presents four main cybersecurity capabilities as listed in Table 52.

Capabilities	Description
Example: Unlinking capability concerning metering dataset Confidentiality, Integrity, Availability Unlinkability, Transparency, Intervenability	Secure hash of PDL (Point de Livraison)
Confidentiality and Authenticity of data	Secured by network protocols (SSH/SSL)
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Logical Access restriction (towards users)	Access to the application is restricted to registered users.
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room).

**TABLE 52 CYBERSECURITY CAPABILITIES OF THE NORDERSTEDT PILOT**

## RISK ANALYSIS

### Threats and breaches identification

This pilot is not using the IF, so it is not directly inherited its analysis, but regarding the threats, they are like the IF analysis but applied to the architecture of the pilot.

#### *Threats*

The 10 threats identified by the IF also correspond to the pilot but applied to its EMS platform.

#### *Breaches*

The pilot has identified 4 breaches, 3 are the same as the breaches identified by the IF but applied to their platform. And the additional one is the bugs and malicious software data breach. The identification of data in bugs of the system or possible malicious software stacks. This breach compromises the integrity of the data and can cause malfunctioning in the system. In general, the impact of this breach will be minor and limited to the ecosystem reputation, citizen privacy. But for the pilot manager will have a significant impact.

### Actionable measures for identified threats

The pilot will use their own measures, which are not very different from the IF, but in this case are applied to the specific architecture of the pilot and nothing is inherited from the IF.

- Information security policies: Data management policies that restrict the circle of persons with access to the systems and only a certain user groups have access to the data.
- Human resource security: During employment, it will be specific training and sensitization. Personnel with access to data are getting aware of the possible threats identified in the analysis.
- Access control: user access and responsibilities management policies where only registered users and authorized ones are granted to certain data.
- Cryptographic controls: Ensure de-identification of datasets and ensure the exchange of data.
- Operation security:

- Operational procedures and responsibilities: it will implement a certificate management and certification of standards (ISMS, BSI...).
- Control of operational software: it uses software only from trustworthy sources.
- Communication security: Information transfer will restrict the communications to only essential information.
- Information security aspects of business continuity management: Information security continuity by setting redundant systems with a backup server for the whole system.
- Compliance: Information security reviews, the pilot will keep valid certificates of software. GDPR and cybersecurity compliance.

**SPP of the pilot is presented in Annex 2.8.1.**

## 10.2 HAMBURG LOCATION

This pilot is in Hamburg, in hotel and commercial locals. The pilot installs a smart charging infrastructure at the hotel to provide a grid compatible and tariff based EV charging infrastructure. The pilot is characterized in Table 53.

<b>Actors</b>	Interoperability framework stakeholder, Pilot manager, User, Service provider	
	Service Provider (Fraunhofer and Uni Kassel)	Both building jointly the communication platform beeDIP which is the coordination unit which connects the DSO with the energy management systems in the field,
	User and data provider SNH	Provides grid measurements and receives grid status information
	Service Provider (Wirelane GmbH)	Provides software to guarantee authentication processes of users and to carry out billing processes. For this purpose, a connection between the charging point and a backend system is established via internet. Furthermore, a charging station is provided which has a charging controller on which the EEBUS software stack is implemented. The scope of use cases to be performed in relation to the software stack is the responsibility of the software stack manufacturer in conjunction with the manufacturer of the charging controller. Wirelane GmbH has no influence on this process.
	Local Flex and security manager (Theben/ KEO)	Gets metering data from the iMSys and provides it to the local EMS and to the grid with the help of the knowledge engine. Gets tariff data and limitation of local power consumption value to the EMS. With the help of the SMGW (Theben) the secure connectivity from DSO to the Hotels will be realized.
<b>Use cases</b>	Variable Tariff Calculation	This service uses grid load predictions (from the DSO), off-shore-wind generation predictions (from the TSO) and spot prices (from the energy exchange) to calculate variable grid fees. Furthermore, the service calculates variable tariffs based on the energy delivery prices (e.g., spot prices) and the given taxes/levies for each customer in addition to the variable grid fees.
	Grid Flexibility Protection Service	This service uses information from forecast schedules and real time measurements in combination with grid topology to estimate current and upcoming grid states. For the state estimation, an ANN-approach is utilized. Based on current and predicted grid states and calculations, possible active power grid flexibilities will be computed within this service.
<b>Architecture entities</b>	Interoperability framework	Enables semantic interoperability for all participating digital platforms, providing energy and non-energy services (control, comfort, and convenience) and devices
	Customer premises	<ul style="list-style-type: none"> <li>• EV Charger</li> <li>• Smart Meter Gateway</li> <li>• Added Value Module</li> <li>• DSO Substation</li> </ul>
	Application	<ul style="list-style-type: none"> <li>• beeDIP backend</li> <li>• Grid Calculation module</li> <li>• Variable Tariff module</li> <li>• EMS-Fair Share Algorithm for Wallboxes</li> <li>• Grid Monitoring Algorithm (TRudi)</li> </ul>

		<ul style="list-style-type: none"> <li>• KEO Prize optimized operation service and Monitoring Grid Connection Point</li> <li>• CPO Backend</li> </ul>
	Application	Applications directly built on top of the semantic interoperability framework instance.

**TABLE 53 CHARACTERIZATION OF THE HAMBURG PILOT**

## 10.2.1 ANALYSIS OF SECURITY AND PRIVACY PROTECTION CAPABILITIES AND RISKS

### Pilot is using the IF

The pilot is using the interoperability framework and is introducing new capabilities as listed in Table 54. While Table 55 gives information about security and privacy protection capabilities of the participating digital platforms.

Capabilities	Description
Example: Unlinking capability concerning metering dataset Confidentiality, Integrity, Availability Unlinkability, Transparency, Intervenability	Secure hash of PDL (Point de Livraison)
Confidentiality and Authenticity of data	Secured by network protocols (SSH/SSL)
Network firewall protection	The network over which all pilot data is communicated is protected by a firewall.
Logical Access restriction (towards users)	Access to the application is restricted to registered users.
Physical access restriction	Access to hardware controlling assets is physically restricted (locked room).

**TABLE 54 CYBERSECURITY CAPABILITIES OF THE HAMBURG PILOT**

Platform name (partner)	Security and privacy protection attributes							
	GDPR compliance	GDPR entity category	Auth Method	API type	API security	IP blocking	Ontology driven security	Access control
Konect (KEO)	Compliant	Controller	SSL	Multiple	Depends on API type	No	No	NA
beeDIP (IEE)	NA/ Only technical data (plant data, power grid data, etc.) is processed and stored	NA/ No personal data is stored, processed, imported or exported	No	REST; MQTT	API Key	No	No	Data/database separated per services

**TABLE 55 - DIGITAL PLATFORMS PARTICIPATING IN THE GERMAN PILOT - HAMBURG LOCATION**

### Threats and breaches identification

This pilot relies on the IF analysis in all the threats, breaches, and their impact in the ecosystem, organisation, and citizens.

#### **Additional threats identified**

There are not additional threats identified.

#### **Additional breach identified**

The pilot inherits the 3 breaches from the IF, and has identified a new one, the bugs and malicious software data breach, with minor overall impact.

The threat number 6 inherited, *User of one interoperable service gets access rights to all interoperable services in the pilot (Elevation of Privilege)* is not possible in the Hamburg pilot for all services. As the pilot has only access to certain services, so the possible breach caused

by this threat will depend on the infiltrated service. It will not affect to this pilot if the infiltrated service is not accessed by the pilot.

The impacts remain almost the same for the system, just the citizen privacy is impacted as maximum in the data breach and limited/significant by the bugs identification breach.

### **Measures for identified threats**

The pilot will use the measures inherited from IF. In this pilot, as it is a more research pilot, the measures of redundancy capabilities, monitoring vulnerabilities and assurance availability to avoid Denial of Service are not considered as the other measures.

### ***Additional actionable measures***

The additional measures to implement are:

- Information security policy: Restricted circle of persons with access to the system, access control.
- Human resource security: During employment, the pilot will provide specific training and sensitization to personnel with access to make them aware of the possible threats.
- Operation security: operational procedures and responsibilities, the project will implement certificate management and certification of standards. Control of operational software by using only software from trustworthy sources.
- Communication security: In the information transfer to enhance a secure transmission, the communication is restricted to the essential information.
- Information security continuity: ensuring the availability of the system by set redundant systems and backup server for the whole system.

**SPP of the pilot is presented in Annex 2.8.2.**

## 11.CROSS ANALYSIS OF PILOTS

This section wraps up the conclusions and provides a birds' eye view of the actionable security and data privacy measures extracted from pilot SPPs. This information is depicted in Table 56.

Pilot	IF	Security & Privacy capabilities	Additional threats	Additional breaches	Additional actionable measures
BE Nanogrid Kobbegem	Yes	Security: Network firewall and authentication (VPN), Physical access restriction	No	No	User access management policy
BE Cordium Hasselt	Yes	Security: Physical access restriction & IT systems restriction.	Non-repudiation Unawareness	No	<ul style="list-style-type: none"> <li>• user access management, physical and assets restrictions, communication security and operation security.</li> <li>• Compliance with legal frameworks.</li> <li>• Regular IT security audits (external service).</li> </ul>
BE Thor Park Genk	Yes	Security: Physical access restriction & IT systems restriction.	Non-repudiation Unawareness	No	<ul style="list-style-type: none"> <li>• user access management, physical and assets restrictions, communication security and operation security.</li> <li>• Compliance with legal frameworks.</li> </ul>
BE Students Tower Antwerp	Yes	Privacy: Confidentiality and authenticity of data. Security: Firewall and Logical and physical access restriction.	No	No	No
BE Nieuwe Dokken	Yes	Security: Network firewall, Two-factor authentication, and Physical access restriction.	No	Business data breach	<ul style="list-style-type: none"> <li>• Access restriction management: minimum accounts, user access policies.</li> <li>• HHRR: during employment training and continuous awareness and preparedness for cybersecurity. Revoke permission when termination and change of employment.</li> <li>• Asset management, user: roles and responsibilities.</li> <li>• Physical and environmental security: Physical key together with registration keys.</li> <li>• Definition of operational procedures (standard and handling of incidents).</li> <li>• Backup: automated database backups for operational and system configuration data.</li> <li>• Logging and monitoring: Network security management: Firewall for the whole network.</li> <li>• Secure transmission over standard secure protocols or password-protected email addresses.</li> <li>• Compliance with legal and contractual requirements: GDPR and cybersecurity compliance.</li> </ul>





BE Zellik Green Energy Park	Yes	Security: Network firewall protection and authentication (VPN access) & physical access restriction.	No	No	User access management: Enforcing the authorised service access.
BE Oud-Heverlee	Yes	Security: Access management policy & Security and data protection: Digital intrusion.	No	No	<ul style="list-style-type: none"> <li>• User access management.</li> <li>• External audits for penetration testing.</li> <li>• Logging and monitoring.</li> <li>• External partner to provide network security and vulnerability scan, assurance of availability of the service and Redundancy in the system.</li> </ul>
BE Mechelen	Yes	No	No	No	Internal organisation for the data management plan
Greek	Yes	Privacy: Unlinking capability concerning metering data set – secure PDL and anonymized metering dataset.	No	No	<ul style="list-style-type: none"> <li>• Internal cybersecurity preparedness during employment.</li> </ul>
Dutch	Yes	Privacy: Unlinking capability concerning metering data set – secure PDL.	Unawareness	No	<ul style="list-style-type: none"> <li>• Human resource security: During the employment (Internal &amp; external cybersecurity preparedness):</li> <li>• Asset management: define the responsibility of assets and the information classification.</li> </ul>
French	Yes	Privacy: Unlinking capability concerning metering data set – secure PDL and Protect against network attacks.	No	No	No
Portuguese	Yes	Security: Secure protocols, Data segmentation, User access control, Resource monitoring and architecture and data management.	No	No	<ul style="list-style-type: none"> <li>• Minimize meaningful and necessary data via the interoperable interfaces.</li> <li>• GDPR and cybersecurity compliance to be done by establishing rules for each privacy boundary by each service stakeholder.</li> </ul>
Italian	Yes	Security: Secure lifecycle of services, Secure instantiation of services, Secure access to services, Integrity of interaction on semantic IF, Protection of assets used or accessed through semantic IF and Logging and monitoring performance of interoperability framework instances.	No	No	<ul style="list-style-type: none"> <li>• User access policies documented.</li> <li>• Asset management: Data governance for employees (responsibilities, termination and change of employment)</li> <li>• Cryptography: For all data storage, all PII to be removed or encrypted.</li> </ul> <p>Physical and environmental security: Protection from malware, Logging will be secure and timestamped, transparency in operations.</p> <ul style="list-style-type: none"> <li>• Network security.</li> <li>• Test data, for this it must have data sharing contracts.</li> <li>• Information security incident management.</li> </ul>
Cross-border	Yes	Security: Secure communication between the cyberGRID platform and the flex providers and hashing the operation data.	No	No	No
GE Norderstedt	No	Privacy: Unlinking capability concerning metering data set – secure PDL, Confidentiality and authenticity of data Security: Firewall and Logical & physical access restriction.	No	No	<ul style="list-style-type: none"> <li>• Information security policies: access data management policies.</li> <li>• Human resource security: During</li> <li>• Cryptographic controls: Ensure de-identification of datasets and ensure the exchange of data.</li> <li>• Operation security:</li> </ul>

					<ul style="list-style-type: none"> <li>○ Operational procedures and responsibilities: it will implement a certificate management and certification of standards (ISMS, BSI...).</li> <li>○ Control of operational software: it uses software only from trustworthy sources.</li> <li>• Communication security: Information transfer will restrict the communications to only essential information (e.g., no small talk).</li> <li>• Redundancy and backup.</li> <li>• Compliance: Information security reviews, the pilot will keep valid certificates of software. GDPR and cybersecurity compliance.</li> </ul>
GE Hamburg	Yes	Privacy: Unlinking capability concerning metering data set – secure PDL, Confidentiality and authenticity of data. Security: Firewall and Logical & physical access restriction.	No	No	<ul style="list-style-type: none"> <li>• Information security policy: user access management policies.</li> <li>• Human resource security: During employment, the pilot will provide specific training and sensitization to personnel with access to make them aware of the possible threats.</li> <li>• Operation security: operational procedures and responsibilities, the project will implement certificate management and certification of standards. Control of operational software by using only software from trustworthy sources.</li> <li>• Communication security: secure transmission, the communication is restricted to the essential information (e.g., no small talk).</li> <li>• Redundancy and backup.</li> </ul>

**TABLE 56 SECURITY AND PRIVACY CROSS ANALYSIS OF PILOTS**

The uptake for the content of this document is to provide a cross analysis and recommendation for pilots. This establishes the ultimate **actionable** set of measures for pilots to consider when deploying, updating or whenever some of the services and systems undergo a major revision. Table 56 summarizes the pilot's security and privacy risk analysis results at this stage of the project. All pilots, except the Norderstedt one, use the IF, which implies that they inherit the results of its analysis (threats, breaches, and measures).

It is clearly shown that most of the cybersecurity capabilities of the pilots are oriented to security, except for those who need to preserve the personal data from the metering point, called PDL (Point de livraison – Point of Delivery).

The most important security capabilities are always the ones to secure the network and secure the data exchange along the network (e.g., Firewall, authentication, VPN access from external network). All these capabilities are reinforced with access restrictions and user access management, sometimes physical restrictions to asset areas only to the authorized personnel.

The privacy capabilities are oriented to anonymize and unlink the PDL from the data subject. Even though anonymized data is not personal data, it is possible to link the data subject to his metering data sets. Unlinking capability takes importance due to this reason.

It is interesting to highlight that the common additional measures identified by the pilots are:

- User access management and responsibilities policies: restrictions, minimum number of users granted access to data, user roles and responsibilities.
- Physical and environmental security: It is applied to the assets, the responsibilities and personnel restriction access (e.g., locked rooms for the assets, electronic keys for authorized personnel registered).
- Human resources management: in and outward employee's policies (e.g., revoke permissions, accounts, or training to aware of the threats and controls of the system).
- Network and operational security: ensure communications, cryptography controls, redundancy, and logging controls.
- Compliance: GDPR, legal framework and cybersecurity standards.

As per **recommendation for security and data protection, pilots should ensure, for all its components, services, and sub-services the following measures proposed by the T5.4 team:**

- All data in transit must be protected by sending it only via secure channels, adopting cryptographically encrypted channels with protocols such as TLS with certificates with long key construction. This should also apply to all APIs exposed to other services via their software controllers or hosting servers.
- While at rest, operational data and metadata persistently stores in database systems, filesystems or other persistent mediums used by services, should encrypt the connections to the database engine system and cumulatively consider the previous measure.
- All hosting platforms, of any sort and location, if in direct control of the pilots should provide a secure environment (as in the previous measures) and consider all the good practices in terms of applying restrictions to the hardware (physically and via remote access) and to software systems. Particularly for physical hardware, identified to be critical to the operation, it should be protected also with restrictions and access policies to physically access the hardware.
- Other organizational principles should be in place as per this recommendation, namely managing employee roles, responsibilities and granted access in a periodic manner. This ensures that unauthorized personnel are granted access by lack of updated credentials.
- In terms of data privacy, pilots should make all efforts to anonymize, obfuscate or clear access policies to personal data from private or corporate users. This is in line with GDPR and does not preclude undergoing through all stages for GDPR compliance. Moreover, pilots and their service owners should always put in question the real need to use and exchange (via the interoperability framework or through other means) users' data. All measures for ensure Privacy-by-design operation should be put in place during design and re-assessed in every major revision of software component.

## 12.CONCLUDING REMARKS

### *What was the purpose of this document?*

This deliverable introduces the complete process for defining actionable security and privacy protection plans (SPP) for the project pilots as well as for the InterConnect interoperability framework as one of the main building blocks of each pilot. This version of the deliverable shows overall progress in defining SPPs for the pilots and the interoperability framework showcasing progress in pilot negotiations and alignment as well as progress in implementing the interoperability framework with respect to maturity of the security and privacy protection capabilities and approaches.

The deliverable is structured to introduce the methodology for collecting inputs from the project pilots on their security and privacy protection plans, capabilities of the participating digital systems and identification of threats and corresponding measures. Then it goes into detailing security and privacy protection capabilities of the InterConnect interoperability framework. All risks, threats and measures are identified and properly documented for the interoperability framework. The deliverable presents different deployment options of the interoperability framework and their impact on privacy and security decision making process behind the project pilots. The SPP of the interoperability framework is introduced as one of the main inputs for pilots to use it as basis for drafting pilot specific SPPs.

Next, the deliverable presents security and privacy protection capability and risks analysis report for each project pilot. These reports are based on templates filled by the project pilots (introduced in the document Annexes). For each pilot a set of capabilities, risks and measures complementing those of the interoperability framework are presented.

### *How were the SPPs created?*

First there was a process of creating suitable templates for collecting all the inputs for constructing the actionable SPPs. These templates were also used to guide the decision-making processes when developing the interoperability framework security and privacy protection capabilities. Also, these templates guided the negotiation and integration processes of the pilots on all levels (technical, policy and business levels). To produce the templates, the Task 5.3 team had to analyse and assess best practices and standard approaches for creating security plans privacy plans and conducting threat and risk analysis from perspective of security and privacy. Major input into the process as work conducted on SPOCS template specification in WP2/D2.2 [1].

After the templates were defined, the Task 5.3 team organized a series of workshops with the project pilot teams as well as with the team working on specification and implementation of the InterConnect interoperability framework. During these workshops the logic behind the templates and overall approach for constructing and utilizing the SPPs were presented. The pilot teams and interoperability framework development team proceeded with filling in the templates and aligning their decision-making processes with the presented SPP best practices in two main stages:



1. Stage 1 – pilots proceeded with specification of their SPPs based on the composition of the interoperable ecosystems they were building. The limitations and capabilities of the participating digital systems were assessed and integration challenges and their impact on security and data protection were documented. At this stage the first draft of the interoperability framework SPP was prepared, which included plans for introducing security and data protection measures into the fabric of the new framework to be developed.
2. Stage 2 – was conducted when both the interoperability framework and pilots achieved higher level of technical and operational maturity. First, the SPP of the interoperability framework was finished detailing all capabilities, threats, risks, and actionable measures to be taken when deploying the framework for achieving syntactic and semantic interoperability. The interoperability framework SPP was then provided as key input to the pilot teams who proceeded with further development of pilots' SPPs. During this stage pilots focused on conducting security and privacy risk analysis, considering the security and privacy capabilities of the InterConnect interoperability framework to validate the security and privacy measures and update their security and privacy plan making it ready for realization/pilot deployment.

### ***What are the main components of a SPP?***

Each pilot SPP, as well as the interoperability framework SPP comprise:

- governance management plan,
- data management plan,
- risk management plan,
- engineering management plan,
- citizen management plan.

These plans are accompanied with:

- Complete list of all security and privacy protection capabilities. The plots using the interoperability framework start with the set off documented capabilities of the framework and add additional capabilities specific to the pilot ecosystem and digital systems participating in its creation.
- List of identified security and privacy protection threats and risks. The pilots base their threat and risk analysis on the threats defined for the interoperability framework as well as threats and risks inherited from the digital systems that comprise the pilot.
- For all threats and risks there is an impact analysis which indicate the severity or criticality of the identified threat/risk for the pilot ecosystem.
- Finally, a set of precise measures for threat/risk handling and mitigation is prepared for each pilot. The interoperability framework threats are addressed by specific set of measures that pilots need to comply with when deploying the framework. There are additional measures for the new/additional threats specific for the pilot ecosystems.

### ***How will the SPPs be utilized within the project?***

The project is proceeding with deployment of the project pilots and instantiation of the interoperability framework within the pilots. This process will rely heavily on the defined SPPs as source of guiding principles when making practical decisions.

SPPs of the pilots are working, live documents. Table 57 shows the overall maturity of developed SPPs per pilot. It indicates that there is still work to be done within the pilot teams to negotiate and agree on proper plans to be included in the SPPs. The level of details provided in SPPs depends on the current stage of the pilot development and general scale of the planned activities (some pilots are very limited in scale and do not involve citizens while others are large scale with plans to involve citizens). Each row in the table corresponds to specific (sub)pilot and its corresponding SPP and columns represent distinct management plans of the SPP. The meaning of metrics for SPP completeness:

- **Advanced** – meaning that the pilot team provided enough details and concrete plans for specific component of the SPP answering most (if not all) of the questions and management plan components. In the subsequent activities, pilots can refine the provided plans.
- **Started** – meaning that pilot team started discussing and agreeing on certain aspects of the management plan while other aspects are still not specified and discussed. Pilot teams will work on finalizing management plan details in the subsequent activities in advancing SPP definition and its implementation.
- **TBS (To Be Specified)** – meaning that the pilot team is still to start discussing and agreeing on the details of the management plan. Some pilots are in early stages of development and after they advance, they will be able to provide corresponding management plan. Pilot teams will work on finalizing management plan details in the subsequent activities in advancing SPP definition and its implementation.
- **NA (Not Applicable)** – meaning that specific management plan is not needed for the pilot. This mostly impact the Citizen Management Plan as some of the pilots are not involving citizens in their planned activities. If the pilot's plans are changed towards inclusion of citizens, the corresponding management plan will be provided in the pilot's SPP.

Pilot name	Governance MP	Data MP	Risk MP	Engineering MP	Citizen MP
Belgium - Nanogrid Kobbegem (section 3.1)	Advanced	Started	TBS	TBS	NA
Belgium – Cordium Hasselt (section 3.2)	Started	Started	Started	TBS	TBS
Belgium – Thor Park Genk (section 3.3)	Started	Started	Started	TBS	Started
Belgium - Students Rooms Tower Antwerp (section 3.4)	Advanced	Started	TBS	TBS	TBS
Belgium - Smart District Nieuwe Dokken Gent (section 3.5)	Advanced	Started	Started	Started	Advanced
Belgium - Zellik Green Energy Park Brussels (section 3.6)	Advanced	Started	Started	TBS	NA
Belgium - Oud-Heverlee Public Buildings (section 3.7)	Advanced	Started	Started	TBS	Advanced
Belgium – Mechelen (section 3.8)	Advanced	Started	Started	TBS	Started
Greek pilot (section 4)	Advanced	Advanced	Advanced	Advanced	Advanced
Dutch pilot (section 5)	Advanced	Advanced	Advanced	Advanced	Advanced
French pilot (section 6)	Started	Advanced	Advanced	Started	Advanced
Portuguese pilot (section 7)	Advanced	Advanced	Started	Started	Started
Italian pilot (section 8)	Advanced	Advanced	Started	Advanced	Advanced
Cross border interoperability pilot (section 9)	Started	TBS	TBS	TBS	TBS
Germany: Residential Pilot Norderstedt (section 10.1)	Started	Started	TBS	TBS	NA
Germany: Commercial Pilot Hamburg (section 10.2)	Started	Started	TBS	TBS	NA

**TABLE 57 - OVERVIEW OF COMPLETENESS OF PILOTS' SPPS AS PRESENTED IN THIS DELIVERABLE**

As the use cases are being implemented and new relationships established, the management plans will evolve. Business and exploitation potential of the pilots and their results directly



depend on properly executed SPPs. Pilots will perform periodic updates and alignments and inform the consortium about the SPP evolution when necessary.

The interoperability framework SPP will be maintained and updated as the framework is validated in the pilot deployments and feedback is received. The feedback and inputs from the wider public (including the cascade funding programs) will also be considered. The received feedback will be parsed and all requirements and issues corresponding to security and privacy protection capabilities and threats will be identified and properly introduced into the framework's SPP.

The project tasks responsible for monitoring pilot execution will assess SPPs in different stages of their development. A set of pilot monitoring KPIs is focusing on security and privacy protection measures applied and reported. These KPIs will rely on the established SPPs as the main inputs for proper characterization and contextualization of the reported pilot results.

### ***How will wider public benefit from the SPPs?***

The complete methodology, templates and lessons learned from the SPP drafting process can be exploited outside of the project itself. The methodology is presented in public deliverables where empty templates are documented as well as proper execution process. The pilot and interoperability framework SPPs can be used as examples. The methodology is specifically well tailored for all projects and initiatives that call for establishing system of systems. During the project lifetime the SPPs and the methodology will be validated in their ability to setup, guide and maintain security and privacy aspects of large-scale cross domain pilots. All shortcomings of different approaches and decisions will be documented and used as lessons learned and success stories accompanying the SPP methodology. All future Horizon projects tackling the challenges of cross domain interoperability and ecosystem building (system of systems) can apply the methodology documented in this (and other) project deliverables.

The pilot and interoperability framework SPPs will be one of the key inputs for the cascade funding projects. They will need to consult the SPPs and align with the plans to be able to join ongoing pilots or utilize interoperability framework to build their own pilots. The same goes for all other 3<sup>rd</sup> parties (not just the cascade funding project extensions) that might join the project pilots or utilize the interoperability framework.

Task leader (Trialog) presented the SPP methodology of the InterConnect project on several occasions and the approach was very well received. Presentations have been made, including during the IEEE 7th world forum on internet of things special session on EC projects (<https://wfiot2021.iot.ieee.org/program/plenary-program/>), and in the AIOTI standardisation WG. There is a plan to discuss with ISO/IEC JTC1/SC27 or SC41 a possibility to create a new or impact an existing standard on security and privacy measures to be applied to system of systems ICT approaches.

Finally, proper SPPs are empowering all ecosystem stakeholders including end users. The plans put specific focus on data and privacy protection in cross domain interoperable ecosystems. A well-executed and maintained SPPs ensure that end user privacy protection is always at the forefront of decision-making process and all ecosystem evolutions do not impact the set level of privacy protection.

## REFERENCES

### PROJECT DOCUMENTS

---

- [1] D2.2 Privacy and Security Design Principles and Implementation Guidelines
- [2] D2.1 Secure Interoperable IoT smart homebuilding and smart energy system reference architecture
- [3] D5.1 Concept Design and architecture of the interoperable marketplace toolbox
- [4] D5.2 Data Flow Management
- [5] Grant Agreement 768935
- [6] D1.1 Services and use cases for smart buildings and grids
- [7] D1.2 Mapping between use cases and large-scale pilots

## ANNEX 1. GUIDELINES USED TO CARRY OUT THE SECURITY AND PRIVACY RISK ANALYSIS OF INTERCONNECT PILOTS

Note: this annex is from the H2020 Automat project deliverable D2.5 (Automat Cyber Security Framework)<sup>10</sup>.

### ANNEX 1.1 THREAT IDENTIFICATION: STRIDE AND LINDDUN TABLES

Table 58 and Table 59 list the categories of security threats and privacy threats that are used in this framework to identify threats. STRIDE was proposed by Microsoft<sup>11</sup>. LINDDUN is proposed by KU Leuven<sup>12</sup>.

Threat	Property	Property description
Spoofing	Authentication	The identity of users is established (or you're willing to accept anonymous users).
Tampering	Integrity	Data and system resources are only changed in appropriate ways by appropriate people.
Repudiation	Nonrepudiation	Users can't perform an action and later deny performing it.
Information disclosure	Confidentiality	Data is only available to the people intended to access it.
Denial Of Service	Availability	Systems are ready when needed and perform acceptably.
Elevation of privilege	Authorization	Users are explicitly allowed or denied access to resources.

**TABLE 58: STRIDE SECURITY THREATS CATEGORIES**

Threat	Property		Property description
Linkability	Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.
Identifiability		Anonymity	Hiding the link between an identity and an action or a piece of information
Non-repudiation		Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict

<sup>10</sup> Available at [https://automat-project.eu/sites/default/files/automat/public/content-files/articles/Automat-D2.5\\_Cyber%20security%20framework.pdf](https://automat-project.eu/sites/default/files/automat/public/content-files/articles/Automat-D2.5_Cyber%20security%20framework.pdf)

<sup>11</sup> The STRIDE threat model; [https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx)

<sup>12</sup> LINDDUN privacy threat analysis methodology, <https://www.linddun.org/>

Detectability		Undetectability and unobservability	Hiding the user's activities
Disclosure of information	Security	Confidentiality	Hiding the data content or controlled release of data content
Unawareness	Soft Privacy	Content awareness	User's consciousness regarding his own data
Non-compliance		Policy and consent compliance	Data controller to inform the data subject to the system's privacy policy, or allow the data subject to specify consents in compliance with legislation

**TABLE 59: LINDDUN PRIVACY THREATS CATEGORIES**

## ANNEX 1.2 IMPACT ASSESSMENT GUIDELINE: RISK MODEL AND RISK MAP

Risk models are used to allow for the evaluation of risks<sup>13</sup>. This framework uses the following model:

Privacy risk level	=	Likelihood of breach	X	Impact of breach
--------------------	---	----------------------	---	------------------

Likelihood is the feasibility of a risk to occur, while impact is the magnitude of the risk. The following scale is used<sup>14</sup>:

- Likelihood:
  - Negligible (1): it does not seem possible for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets;
  - Limited (2): it seems difficult for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets;
  - Significant (3): it seems possible for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets; and
  - Maximum (4): it seems extremely easy for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets;
- Impact:
  - Negligible (1): Organisations and users either will not be affected or may encounter a few inconveniences, which they will overcome without any problem;
  - Limited (2): Organisations and users may encounter significant inconveniences, which they will be able to overcome despite a few difficulties;
  - Significant (3): Organisations and users may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties; and

<sup>13</sup> NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012

<sup>14</sup> Reference used is <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>. CNIL PIA manual 1- tools (templates and knowledge bases). Definition has been modified to include both security and privacy aspects.

- Maximum (4): Organisations and users may encounter significant, or even irreversible, consequences, which they may not overcome.

When breach likelihood and a breach impact have been determined, they can be plotted on a risk map. The whole exercise of risk assessment is to reduce the likelihood of threats materialisation to negligible or limited.

Maximum Impact	Must be avoided or reduced		Absolutely avoided or reduced	
Significant Impact				
Limited Impact	These risks may be taken		Must be reduced	
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

TABLE 60: RISK MAP

## ANNEX 1.3 EXAMPLES OF BREACH IMPACT

Table 61 lists examples of impact on user's privacy and on an organisation<sup>15</sup>.

<b>Impact on user's privacy</b>	loss of autonomy exclusion loss of liberty physical harm stigmatization power imbalance loss of trust economic loss
<b>Impact on the operations and business of an organisation</b>	non-compliance costs (i.e., impact on the organization of not complying with applicable laws, policies, contracts); direct costs (e.g., potential for decrease in use of the system or face other impediments to achieving its mission); reputational costs (e.g., negative impact on public trust in the organization); internal culture costs (e.g., negative impact on employee morale, retention, or other aspects of organization culture); and other costs specific to each organization work, mission, structure, and customer base.

TABLE 61: IMPACT EXAMPLES

<sup>15</sup> From NISTIR 8062. "Introduction to Privacy Engineering and Risk Management in Federal Systems". January 2015. [http://csrc.nist.gov/publications/drafts/nistir-8062/nistir\\_8062\\_draft.pdf](http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf)

## ANNEX 1.4 CONTROL CATEGORIES

Table 62 lists the categories of control/measures that can be used to address risks. These categories are used in ISO/IEC 27002 (Code of practice for information security controls), 27552 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines), 29151 (Code of practice for personally identifiable information protection).

Category	Sub-categories
Information security policies	Management direction.
Organization of information security	Internal organisation Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification
Access control	Business requirements of access control User access management User responsibilities System and application access control Media handling
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communication security	Network security management Information transfer
System acquisition, development, and maintenance	Security requirements of information system Security in development and support processes Test data
Suppliers' relationships	Information security in supplier relationships Supplier service delivery management
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity Redundancies
Compliance	Compliance with legal and contractual requirements Information security reviews

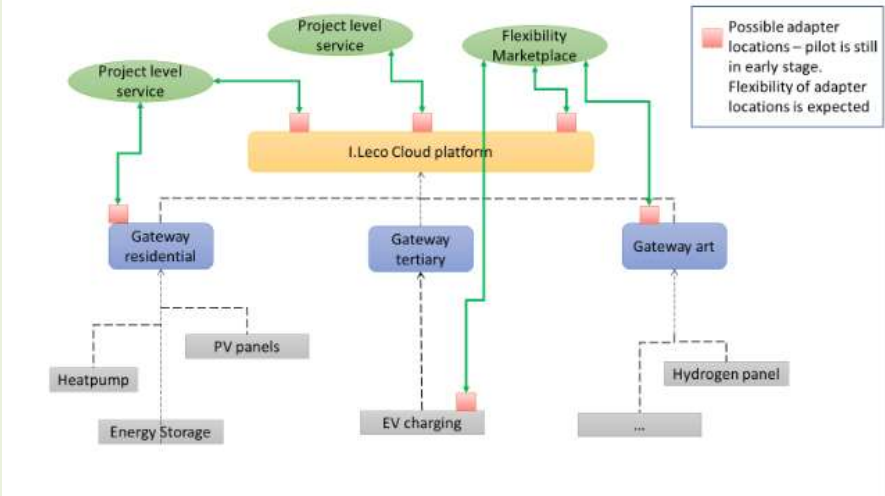
**TABLE 62: CONTROL CATEGORIES**



# ANNEX 2. SECURITY AND PRIVACY PLANS PER PILOT

## ANNEX 2.1 PILOTS IN BELGIUM: SPP

### ANNEX 2.1.1 NANOGRID KOBEGEM (THINK-E)

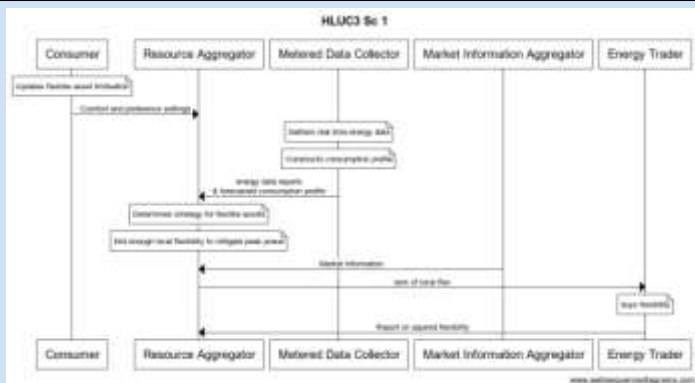
1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	NANOGRID KOBEGEM
SUMMARY	<p><b><u>Scope and objectives</u></b></p> <ul style="list-style-type: none"> <li>Aggregation of Energy in Local Energy Community through local controller with focus on grid interaction: This service provides the maximum amount of flexibility in a neighbourhood by combining all available flexible assets while considering user preferences.</li> <li>Voluntary (non-) participation in Energy Community: This service provides users of a pilot the possibility to connect and disconnect to the energy community. Users of the pilot will have the option to temporarily not participate in the energy and non-energy services of the site.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.1.</i></p>
DESCRIPTION	 <p><b>FIGURE 13: OVERVIEW OF THE NANOGRID KOBEGEM PILOT</b></p> <p>The local controller /aggregator is responsible for aggregating energy and information of the energy community. It is the only connection point to the grid. It is a software platform operator that automates and controls the energy community. This energy community consists in 1 residential two floor apartment, an office, a lab and 2 art installations). All the members of the energy community will be able to (temporarily) disconnect from the energy community. For the pilot, it will be necessary that each member of the community has a variety of devices including:</p> <ul style="list-style-type: none"> <li>AC and DC home appliances.</li> <li>Electrical heating</li> <li>Different ventilation systems</li> </ul> <p>The pilot is a holistic approach towards energy communities: there are several devices which are common to the community especially for energy production and storage.</p> <ul style="list-style-type: none"> <li>PV panels</li> <li>Hydrogen fuel cell</li> <li>EV infrastructure (Vehicle to Grid)</li> <li>Heat pump</li> <li>Stationary battery</li> <li>Hydrogen boiler</li> </ul>

	<ul style="list-style-type: none"> <li>DC grid</li> </ul> <p>These devices need to be able to communicate to the local controller's software platform. Therefore, there is also a need for gateways. The communication protocol between the devices and gateways and between gateways and software platform is not yet defined.</p>
--	---

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		GDPR
International Standards		N/A
2.1	Governance Body	
Information Security Manager		Arnor Van Leemputten
Data Protection Officer		Arnor Van Leemputten
Other roles		N/A
Ecosystem consideration		No, the governance body might change after the InterConnect project.
2.2	Organisation Responsibility	
Entity 1	Entity Name	Th!nk E
	Role	Data processor
	Address	Ophemstraat 140, 3050 Oud-Heverlee, Belgium
	Contact(s)	Arnor Van Leemputten: ( <a href="mailto:arnor@think-e.be">arnor@think-e.be</a> )
	Entity Type	Smart building hard- and software provider
Entity 2	Entity Name	Imtech
	Role	Data controller
	Address	Boulevard Industrielaan 28, 1070 Anderlecht, Belgium
	Contact(s)	Christof De Knop: ( <a href="mailto:christof.de.knop@imtech.be">christof.de.knop@imtech.be</a> )
	Entity Type	Cooperative energy service company (ESCO)
Structure of responsibility		<ul style="list-style-type: none"> <li>Th!nk E: Energy services implementation</li> <li>Imtech: Software platform controller (outside of InterConnect Consortium)</li> </ul>
2.3	Rules and procedure	
Meetings		Taking into consideration that Nanogrid is a small-scale project, small meetings have been organised on both regular and ad-hoc basis between Th!nk E's (Arnor Van Leemputten) and Imtech's (Christof de Knop) representatives.
Nomination		N/A
Publication of minutes		N/A
2.4	Continual improvement and periodic update	
Meetings		Please see 2.3
Evaluation procedure		To be specified.

3	DATA MANAGEMENT PLAN <sub>16</sub>	
InterConnect data management plan is the first input		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data		Th!nk E/ Imtech

<sup>16</sup> The pilot may have two or more applications. The data management plan should be repeated for each application.

PII Controller <sup>17</sup>		Imtech
PII Processors <sup>18</sup>		Th!nk E/ Imtech
PII Principals <sup>19</sup>		One residential building user
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach		Th!nk E and Imtech have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site (including data obtained in the context of InterConnect). The user signed an informed consent form, confirming that his personal data can be used for research (not limited to InterConnect).
Agreement 1	Organizations	Th!nk E/ Imtech
	Agreement template	The agreement between Th!nk E and Imtech is separate from the InterConnect project itself but covers all the required data management processes relevant to InterConnect.
<b>3.2.2 Data description</b>		
Data	Dates for collection	The start of collection of data is planned for Sep 2021
	Identification of data	1. Electricity demand per living unit 2. Asset measurements (battery, heat pump...)
	Type of data	critical to service data
	Life Cycle	According to the informed consent form (see Agreement approach), data obtained can be used for research purposes also beyond InterConnect. Historical data is also used to provide better services. No storage time/deletion process is therefore fixed at this point.
	Data description	To be specified
<b>3.2.3 Data exchange</b>		
Data flow		 <p><b>FIGURE 14: DATA FLOW DIAGRAM FOR PILOT NANOGRID KOBBEDEM</b></p>
Data access control chart		To be specified
<b>3.2.4 Data access monitoring</b>		
Data access verification procedure		Secure access is implemented by VPN to entre externally, also at the IF level
<b>3.2.5 Data Registry</b>		
Registry of agreements		To be specified

<sup>17</sup> ISO/IEC TR 27550 definition: Privacy stakeholder that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

<sup>18</sup> ISO/IEC TR 27550 definition: Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

<sup>19</sup> ISO/IEC TR 27550 definition: Natural person to whom the personally identifiable information (PII) relates

Registry of data sets	<i>To be specified</i>
Registry of citizen consents	<i>They will be stored in a secure environment, locked for the physical files and digitally, they will be kept under restricted access and secured network environment.</i>

#### 4 RISK MANAGEMENT PLAN

As the nature and scale of the pilot is small, there has not been detailed a specific risk management plan. It has been scheduled the risk analysis workshops, led by Trialog, and several internal meetings to finish the risk analysis. As it is well-known, a risk analysis (e.g., DPIA) are also in continuous evolution, they are not static documents, neither the SPP file. They need to be checked and analyse again periodically to be updated more accurate to the needs of the pilot. Therefore, in this deliverable, it is presented some updates in the SPP and the first Security and privacy analysis report, which will be checked and update along the project and beyond it.

#### 5 ENGINEERING MANAGEMENT PLAN

To be specified by the pilot team.

#### 6 CITIZEN ENGAGEMENT PLAN

This pilot does not involve citizens. This is not applicable to the pilot.

### ANNEX 2.1.2 CORDIUM HASSELT (VITO)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	CORDIUM HASSELT
SUMMARY	<p><b><u>Scope and objectives</u></b></p> <ul style="list-style-type: none"> <li>Community optimization of efficient heat generation: The main objective is to maintain District Heating Network costs reduced by optimizing the use of local RES generation, thermal storage, and controllable loads (e.g., controllable HP).</li> <li>Peak saving via direct control of HP: The main objective is to 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.</li> <li>Increase RES for self-consumption: coordination of energy consumption and local renewable generation. The main objective is to maximize consumption of local RES generation (from PVT and wind turbine) at hours of high production to reduce electricity supply costs for heat generation.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>

**FIGURE 15: OVERVIEW OF CORDIUM HASSELT PILOT ARCHITECTURE**

In this use case, there are four buildings with a total of 20 units that are connected via a DHN to two other building clusters. Each cluster (or 'phase') has its own boiler room.

**DEVICES USED:**

- BTES
- PV(-T)
- Thermal substations (DHW buffer 90l) + electric heater
- 1 small wind turbine
- Smart whitegoods
- Apartment sensors/thermostat
- HPs (electric, gas)

<b>2</b>		<b>GOVERNANCE MANAGEMENT PLAN</b>	
Rules and legislation		GDPR	
International Standards		To be specified.	
<b>2.1</b>		<b>GOVERNANCE BODY</b>	
Information Security Manager		Koen Allaerts / Ectors Dominic	
Data Protection Officer		Koen Allaerts / Ectors Dominic	
Other roles		N/A	
Ecosystem consideration		No, i.e., the governance body might change after the InterConnect project	
<b>2.2</b>		<b>ORGANISATION RESPONSIBILITY</b>	
<b>Entity 1</b>	Entity Name	VITO	
	Role	Data Controller	
	Address	VITO NV   Boeretang 200   2400 Mol, Belgium	
	Contact(s)	Koen Allaerts: <a href="mailto:Koen.allaerets@vito.be">Koen.allaerets@vito.be</a> Dominic Ectors: <a href="mailto:dominic.ectors@vito.be">dominic.ectors@vito.be</a> Georg Jung: <a href="mailto:Georg.jung@vito.be">Georg.jung@vito.be</a> Chris Caerts: <a href="mailto:chris.caerts@vito.be">chris.caerts@vito.be</a>	
	Entity Type	Research Organisation	
Structure of responsibility		VITO: responsible for data collection, data storage, data treatment, granting access to the gathered data.	

2.3	Rules and procedure	
Meetings		To be specified.
Nomination		Employees of VITO and Cordium
Publication of minutes		To be specified.
2.4	Continual improvement and periodic update	
Meetings		To be specified.
Evaluation procedure		An evaluation can take place after the third workshop (where the security and privacy analysis are carried out).

3	DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data		Cordium NV, residents
PII Controller		VITO
PII Processors		VITO
PII Principals		Residents
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		Consent form signed by residents (to be checked)
Agreement 1	Organizations	VITO, Cordium
	Agreement template	To be specified
3.2.2	Data description	
Data	Dates for collection	Starting at the fourth quarter of 2021
	Identification of data	1. Site level: RES production measurements 2. Site level: measurements related to district heating network 3. Site level: electricity demand, energy (gas) demand 4. Heat demand per living unit for space heating and for hot water 5. For a small set of apartments (5): occupancy data 6. For a small set of apartments (5): electricity demand per living unit
	Type of data	1. Critical to service data 2. Critical to service data 3. Critical to service data 4. PII/Critical to service data 5. PII 6. PII



	Life Cycle	According to the informed consent form data obtained can be used for research purposes also beyond InterConnect. Historical data is also used to provide better services. No storage time/deletion process is therefore fixed at this point. (to be checked) this. <ul style="list-style-type: none"> <li>Starting date: EV building has been measured from the opening on of the building</li> <li>Storage time: no storage time</li> <li>Deletion process: no deletion process</li> </ul>
	Data description	Timeseries data – To be specified
3.2.3	Data exchange	
Data flow		To be specified.
Data access control chart		To be specified.
3.2.4	Data access monitoring	
Data access verification procedure		A limited number of persons (researchers) has access to the data. Access is granted by VITO admin. Access of a third party (in context of WP8) should be granted having the consent of data owner and principal.
3.2.5	Data Registry	
Registry of agreements		To be specified.
Registry of data sets		To be specified.
Registry of citizen consents		To be specified.

4	Risk Management Plan	
4.1	Pilot needs and resources for security and privacy risk management	
Context for privacy analysis		There is not a systematic and extensive evaluation of the personal aspects of an individual, including profiling; nor processing of sensitive data on a large scale; nor systematic monitoring of public areas on a large scale. So, no DPIA threshold is exceeded.
Context for security analysis		To be specified.
Context for the project		To be specified.
4.2	Risk management process	
4.2.1	Security	
Methodology		To be specified.
Schedule		2nd workshop to be held on May/June 2021
Template		InterConnect template for risk analysis will be provided and used to conduct the analysis.
4.2.2	Privacy	
Methodology		To be specified.
Schedule		2nd workshop to be held on May/June 2021
Template		InterConnect template for risk analysis will be provided and used to conduct the analysis.

## 5 ENGINEERING MANAGEMENT PLAN

The engineering plan has not yet been specified in this pilot, but as the project advances, it will be done in the m4 meeting where the risk and privacy analysis will be performed

## 6 CITIZEN ENGAGEMENT PLAN

To be specified.

### ANNEX 2.1.3 THOR PARK GENK (VITO)

1 SECURITY AND PRIVACY PLAN CONTEXT	
PILOT NAME	THOR PARK GENK
SUMMARY	<p><b>Scope and Objectives:</b></p> <ul style="list-style-type: none"> <li>Manage peak load to avoid increases in the electricity invoice (peak shaving) from table =&gt; Building level services: peak shaving --&gt; reduce electricity invoice</li> <li>Building level services: RES self-consumption --&gt; reduce electricity invoice: The energy service provider forecasts the generation profile of available RES (directly connected to the system in question). This generation profile is matched with the consumption profile of the system.</li> <li>Building level services: EV smart charging pricing for flexibility use. It describes how flexibility from a building/parking lot equipped with EV charging stations and PV panels may be traded in a cost-efficient and cost-reflective.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p><b>FIGURE 16: OVERVIEW OF THE THOR PARK GENK PILOT ARCHITECTURE</b></p> <p>This use case is set for office buildings and parking, energy efficiency in parking and offices to offer employees. It tries to offer flexibility but also peak energy shaving to the users. As there is parking involved, there are different devices: EVs, PV panels, BEMs, SmartThor platform.</p> <p>In this use case, there is a variety of actors, from the Prosumer (EV user/owner to market operator, building/parking manager, energy service provider, forecaster, technical aggregator through InterConnect Interoperability framework and DCM BEMs platform).</p> <p>In summary, there are many different applications connected through a platform to offer different services to users to reach the three main objectives depicted in the row above.</p>

2 GOVERNANCE MANAGEMENT PLAN	
Rules and legislation	GDPR
International Standards	Not specified
2.1 GOVERNANCE BODY	
Information Security Manager	Wim Cardinaels /Ectors Dominic

Data Protection Officer		Wim Cardinaels /Ectors Dominic
Other roles		N/A
Ecosystem consideration		No, the governance body might change after the InterConnect project.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	VITO
	Role	Data Controller
	Address	VITO NV   Boeretang 200   2400 Mol, Belgium
	Contact(s)	Wim Cardinaels: <a href="mailto:wim.cardinaels@vito.be">wim.cardinaels@vito.be</a> Dominic Ectors: <a href="mailto:dominic.ectors@vito.be">dominic.ectors@vito.be</a> Georg Jung: <a href="mailto:Georg.jung@vito.be">Georg.jung@vito.be</a> Chris Caerts: <a href="mailto:chris.caerts@vito.be">chris.caerts@vito.be</a>
	Entity Type	Research Organisation
Structure of responsibility		VITO: responsible for data collection, data storage, data treatment, granting access to the gathered data. KU Leuven also is involved in this pilot.
2.3 Rules and procedure		
Meetings		To be specified: in mean time monthly meetings with Genk municipality and Thor NV.
Nomination		Employees of VITO, Genk, and Thor NV
Publication of minutes		To be specified.
2.4 Continual improvement and periodic update		
Meetings		To be specified.
Evaluation procedure		To be specified.

3	DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data		Building owner (EnergyVille1, Incubathor)
PII Controller		VITO
PII Processors		VITO
PII Principals		EV drivers
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		Friendly users have been recruited and have given their agreement (mail) to participate in the experiment, not to share their data with 3rd parties.
Agreement 1	Organizations	VITO/KU Leuven, building owners.
	Agreement template	Old data has been collected under NDA. New contracts are being negotiated.
3.2.2	Data description	
Data 1	Dates for collection	Fourth quarter of 2021 for InterConnect (collection of historical data started at 2016 for the EnergyVille1 building, for the other buildings in the park now they will be connected to the system.)

	Identification of data	1. EV vehicle arrival time, target departure time, energy required at departure time, person & EV identification & profile. 2. Building energy consumption 3. Building RES production
	Type of data	1. PII/Critical to service data 2. Critical to service data 3. Critical to service data
	Life Cycle	Starting date 2016 (buildings joining). No scheduled storage time /deletion process. Every data owner can request to delete its data.
	Data description	Timeseries data – To be specified
3.2.3	Data exchange	
	Data flow	<i>To be specified.</i>
	Data access control chart	<i>To be specified.</i>
3.2.4	Data access monitoring	
	Data access verification procedure	A limited number of persons (researchers) have access to the data. Access is granted by VITO admin. Access of a third party (in context of WP8) should be granted having the consent of data owner and principal. Upgraded procedure to be developed.
3.2.5	Data Registry	
	Registry of agreements	<i>To be specified.</i>
	Registry of data sets	<i>To be specified.</i>
	Registry of citizen consents	<i>To be specified.</i>

4	<b>RISK MANAGEMENT PLAN</b>	
4.1	Pilot needs and resources for security and privacy risk management	
	Context for privacy analysis	There is not a systematic and extensive evaluation of the personal aspects of an individual, including profiling; nor processing of sensitive data on a large scale; nor systematic monitoring of public areas on a large scale. So, no DPIA threshold is exceeded.
	Context for security analysis	<i>To be specified.</i>
	Context for the project	<i>To be specified (see Context for privacy analysis).</i>
4.2	Risk management process	
4.2.1	Security	
	Methodology	To be specified, external security audit is planned.
	Schedule	2nd Workshop in May/June 2021.
	Template	Use the InterConnect template.
4.2.2	Privacy	
	Methodology	<i>To be specified.</i>
	Schedule	2nd Workshop in May/June 2021.
	Template	Use the InterConnect template.

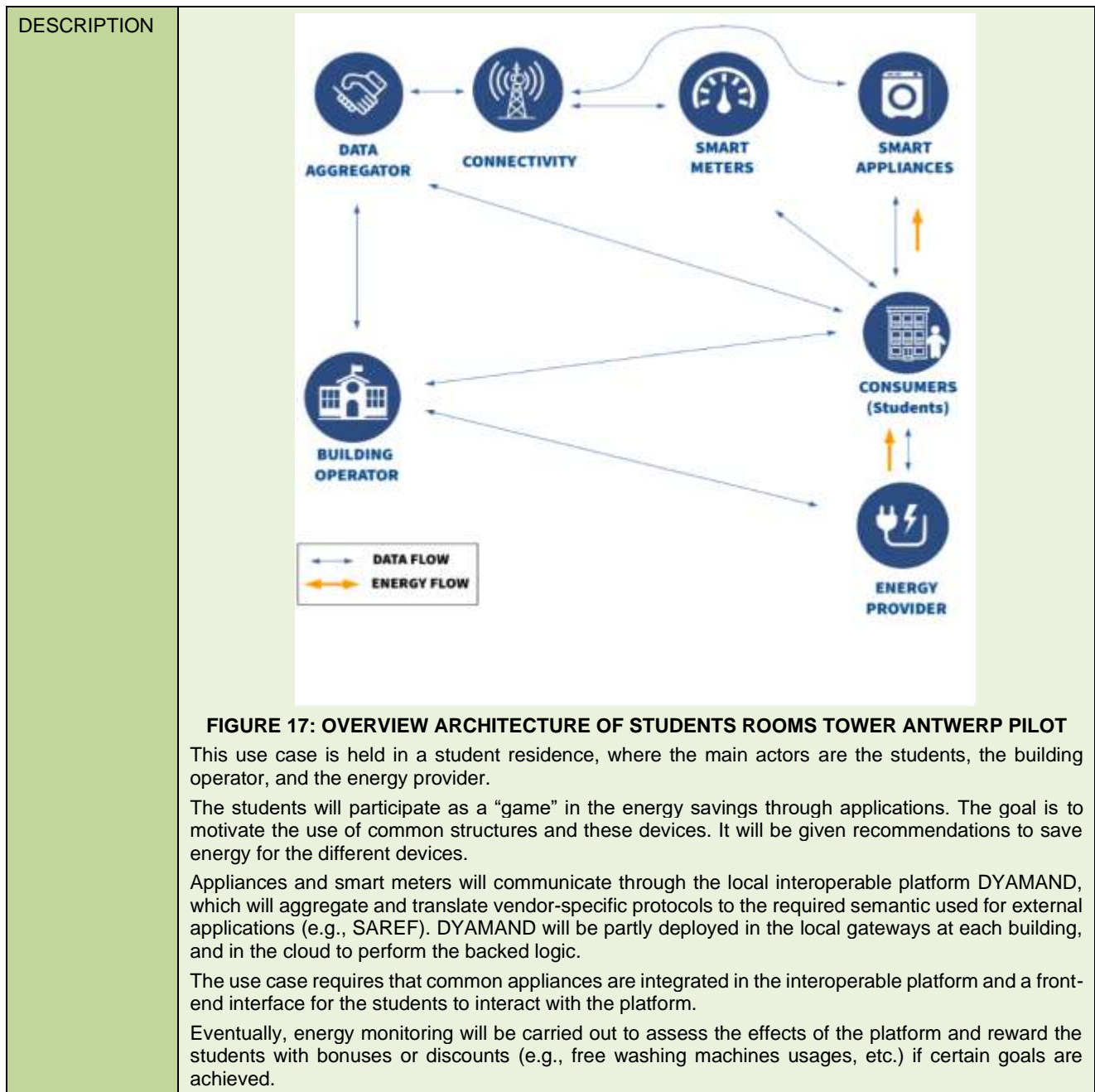
## 5 ENGINEERING MANAGEMENT PLAN

To be specified until the m4 meeting.

6	CITIZEN MANAGEMENT PLAN
Pilot needs and resources for management	Friendly users (EV owners) are EnergyVille and VITO personnel charging their privately owned or company car for free at EnergyVille. Friendly users are engaged to participate in the experiment.
Management process	Participants get feedback via the app and can overrule settings. A contact person is assigned. Experiment feedback is given in regular intervals.
Schedule	<i>To be specified.</i>

## ANNEX 2.1.4 STUDENTS ROOMS TOWER ANTWERP (IMEC)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	STUDENTS ROOMS TOWER ANTWERP
SUMMARY	<p><b><u>Scope and Objectives:</u></b></p> <ul style="list-style-type: none"> <li>• “Gamification” of the use of common appliances.</li> <li>• Building operators are usually interested on having an energy profile as flat as possible. This helps DSOs and TSOs to better manage the grid, avoiding dealing with constant fluctuation in the demand curve. To achieve a flat consumption curve, building operators can leverage consumption patterns and gamified usage of appliances by the students to flatten the curve reduce management costs.</li> <li>• Common appliances (e.g., like shared white goods in a student residence building) can be intelligently used, optimizing capacity, and scheduling its active times beforehand to minimize activity time during grid peak hours and encouraging its use in valley hours. This will be done by engaging students in a “collaborative game” where they will get benefits (e.g., discounts within the building) for a responsible and efficient usage of common appliances.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>



2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		GDPR
International Standards		N/A
2.1 GOVERNANCE BODY		
Information Security Manager		Esteban Municio
Data Protection Officer		Esteban Municio
Other roles		N/A
Ecosystem consideration		To be specified.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	Imec - Universiteit Antwerpen, Lammp (not an InterConnect partner)



	Role	Data processor, data controller
	Address	The Beacon, 7th floor Sint-Pietersvliet 7 2000 Antwerpen
	Contact(s)	Esteban Municio: <a href="mailto:esteban.municio@uantwerpen.be">esteban.municio@uantwerpen.be</a> Johann Marquez Barja: <a href="mailto:Johan.marquez-barja@uantwerpen.be">Johan.marquez-barja@uantwerpen.be</a>
	Entity Type	Research group of the University of Antwerp and imec, Lammp is not an InterConnect partner.
Structure of responsibility		Imec – University of Antwerp: data storage, data treatment Lammp: granted access to gathered data, not held responsible for technical protection of the data.
2.3	Rules and procedure	
Meetings		A meeting regarding data and data policies will be held every year. The first meeting will be held before the initial installation of smart meters.
Nomination		The employees of Imec - University that are most relevant to security issues will convene during the governance body meetings.
Publication of minutes		To be specified.
2.4	Continual improvement and periodic update	
Meetings		A meeting regarding data and data policies will be held every year.
Evaluation procedure		An evaluation can take place after the 3rd workshop (where security and privacy analysis are carried out).

3		DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.			
3.1		Pilot needs and resources for security and privacy data management	
Ownership of data		Imec – University of Antwerp	
PII Controller		Imec – University of Antwerp	
PII Processors		Imec – University of Antwerp, Lammp	
PII Principals		Students living in the building	
3.2		Data Management Process	
3.2.1		Agreements	
Agreement approach		Before the pilot starts, Imec – University of Antwerp and Lammp will sign a mutual agreement, regarding the controlling and processing of personal data on the pilot site (including data obtained in the context of InterConnect). The students living in the building are the producers of data and will sign an informed consent form, confirming that their personal data can be used for research (not limited to InterConnect).	
Agreement 1	Organizations	Imec – University of Antwerp, Lammp	
	Agreement template	The agreement template needs still to be built. The agreement between Imec – University of Antwerp and Lammp is separate from the InterConnect project itself but will cover all the required data management processes relevant to InterConnect.	
3.2.2		Data description	
Data	Dates for collection	September 2021 for energy consumption readings. September 2022 for statistics over collaborative usage. September 2022 for grid forecast data.	

Identification of data	<ol style="list-style-type: none"> <li>1. Readings of aggregated energy consumption as per floor in the building.</li> <li>2. Statistics over collaborative usage of common appliances, aggregated.</li> <li>3. Grid forecast data (not personal data, supplied by a forecaster).</li> </ol>
Type of data	Critical to service data.
Life Cycle	<p>Data can be used for research purposes beyond InterConnect. Also, historical data can be used by Lammp to optimize the management of the building. Students will be able to track their collaborative energy consumption (aggregated) to follow the evolution of the “game”</p> <p>No storage time/deletion process is therefore fixed at this point.</p>
Data description	<i>To be specified.</i>

### 3.2.3

#### Data exchange

##### Data flow

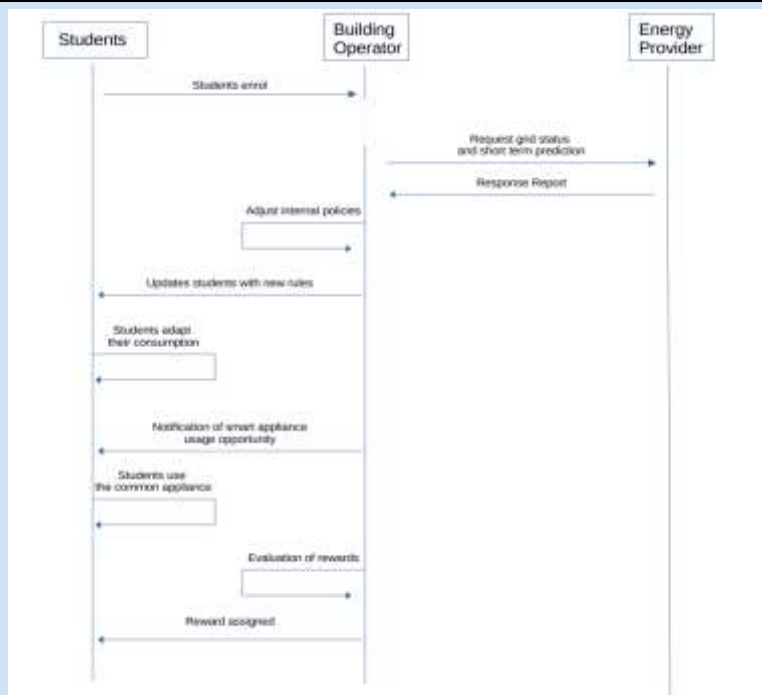


FIGURE 18: DATA FLOW DIAGRAM OF STUDENTS ROOMS TOWER ANTWERP PILOT

##### Data access control chart

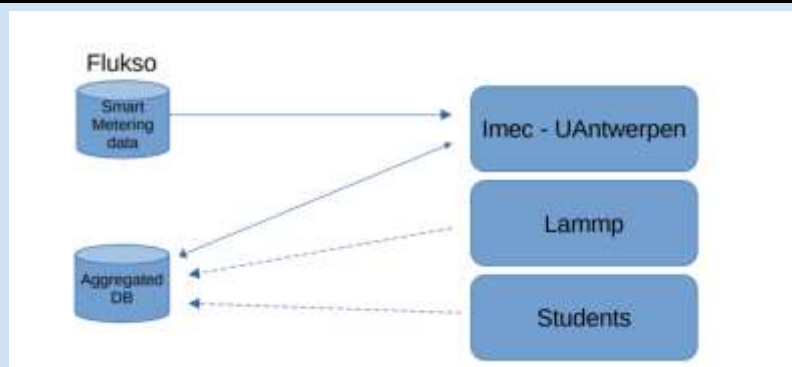


FIGURE 19: DATA ACCESS DIAGRAM

### 3.2.4

#### Data access monitoring

##### Data access verification procedure

Third party actors (i.e., Lammp) will have access granted having the consent of data owner and principal.

### 3.2.5

#### Data Registry

##### Registry of agreements

*To be specified.*

##### Registry of data sets

*To be specified.*

Registry of citizen consents	To be specified.
------------------------------	------------------

#### 4 RISK MANAGEMENT PLAN

This is a small pilot in public buildings, for that reason the security and privacy needs are minimal, and it is not specified a plan now. The plan will be specified until the m4 meeting.

#### 5 ENGINEERING MANAGEMENT PLAN

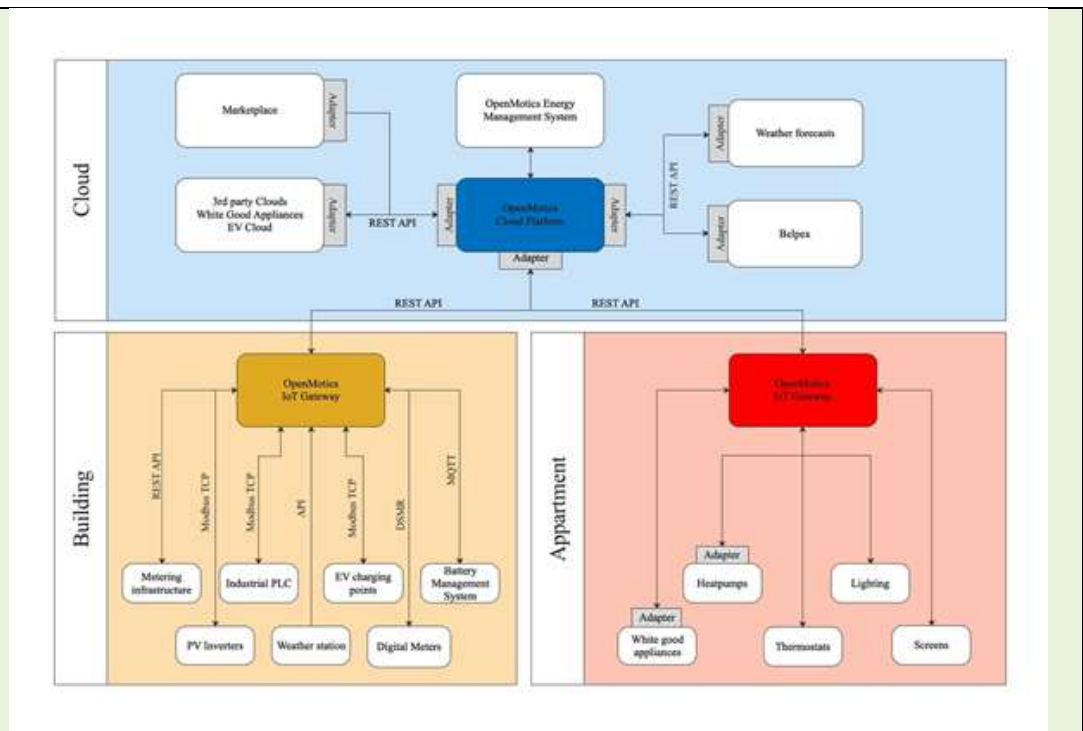
This is a small pilot in public buildings. The engineering management plan is not yet specified. The plan will be specified until the m4 meeting.

#### 6 CITIZEN ENGAGEMENT PLAN

This is a small pilot in public buildings. The citizen management plan may not be needed, so it is not relevant for the project. The plan will be specified until the m4 meeting.

### ANNEX 2.1.5 SMART DISTRICT NIEUWE DOKKEN GENT (DUCOOP)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	SMART DISTRICT NIEUWE DOKKEN GENT
SUMMARY	<p><b><u>Scope and Objectives:</u></b></p> <ul style="list-style-type: none"> <li>DuCoop (www.ducoop.be) is pioneering in the Belgian and European market for developing new technologies and designs for smart and sustainable districts based on decentralized wastewater treatment and integrated recovery of waste heat, resources (water, nutrients) and renewable electricity.</li> <li>During the InterConnect-project, DuCoop will manage and operate a large residential Local Energy Community in Ghent, bringing smart Energy IoT-appliances into practice in a real-life environment. DuCoop already interacts with the other partners in this pilot, i.e., Imec and OpenMotics. Within this project also the further alignment with STORM, on matching the energy consumption with the excess wind energy, and Farys Solar, on matching with a local large PV set-up, is elaborated.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p>The loads of collective appliances (district heating network (pumps), EV-charging infrastructure, District battery storage, (vacuum) sewage system pumps, water treatment plant etc.) are monitored and controlled by an EMS system that is managed by the sustainability cooperative DuCoop that manages energy and sustainability services in the district.</p> <p>Interaction between neighbourhood and individual households (smart appliances in houses). In the framework of grid balancing on district level (e.g., local DSO-connection) DuCoop has created a home automation network (in cooperation with OpenMotics) that allows monitoring of energy, water, etc. consumption and smart appliances in the individual houses. This End-user platform can be used to create interactions between individual energy consumers and the collective EMS, grid balancing agents, potential 3rd party services, etc.</p> <p><b>Data</b></p> <ul style="list-style-type: none"> <li>Real time consumption and production data in the district (industrial/end-user level)</li> <li>Local and regional grid balancing data (TSO/DSO)</li> <li>Meteo data and prediction models for consumption behaviour and local RES-production</li> <li>Model data from Battery management and local Energy management system.</li> </ul>



**FIGURE 20: OVERVIEW ARCHITECTURE OF NIEUWE DOKKEN GENT PILOT**

**Cross-platform interoperability challenges**

- Technology issues: readiness level, affordability, usage complexity.
- Eagerness of end-users to be involved (what's in it for them?).
- What are the incentives for end-users to share their data/influence their behaviour/living comfort?
- Legal aspects: use of end-user data, tariff schemes, energy, and climate policies (RES).
- Scalability: what size is attractive to the market?
- Data frequency differences in between platforms/assets.
- When using many assets to become interoperable, interoperability might increase complexity quite a lot.

**Cross-platform interoperability possible solutions**

- Local sustainability cooperative: creating awareness with end-users. Short follow-up of concerns.
- Interoperability can reduce complexity of technologies and applications.
- Valorising extra added value (local RES, overall sustainability of the housing projects, optimization of grid and IT-infrastructure, energy efficiency).
- Proof of concept can stimulate innovative policy schemes.
- Documentation.

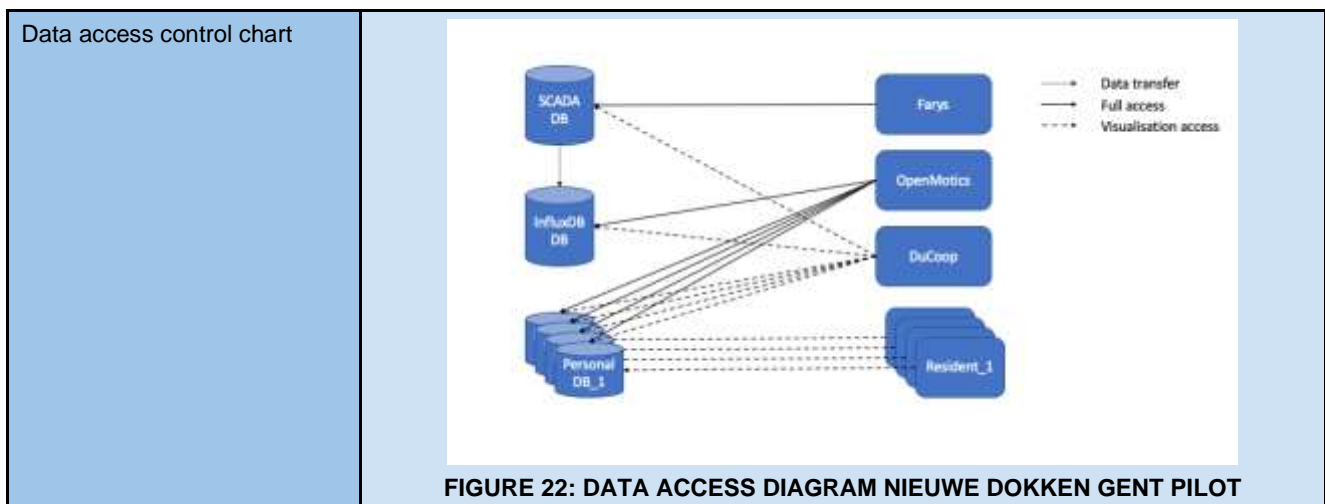
2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		GDPR
International Standards		N/A
2.1 GOVERNANCE BODY		
Information Security Manager		Chaïm De Mulder
Data Protection Officer		Chaïm De Mulder
Other roles		N/A
Ecosystem consideration		No, i.e., the governance body might change after the InterConnect project.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	OpenMotics
	Role	Data processor

	Address	Vlasgaardstraat 52, 9000 Gent, Belgium
	Contact(s)	Chaïm De Mulder <a href="mailto:chaim.de.mulder@openmotics.com">chaim.de.mulder@openmotics.com</a> (for DuCoop also)
	Entity Type	Smart building hard- and software provider.
Entity 2	Entity Name	DuCoop
	Role	Data controller
	Address	Poortakkerstraat 94, 9051 Sint-Denijs-Westrem, Belgium
	Contact(s)	Chaïm De Mulder: <a href="mailto:chaim.de.mulder@openmotics.com">chaim.de.mulder@openmotics.com</a>
	Entity Type	Cooperative energy service company (ESCO)
Entity 3	Entity Name	Farys
	Role	Data Processor
	Address	Stropstraat 1, 9000 Gent, Belgium
	Contact(s)	Not a partner of InterConnect project (Contact Chaïm De Mulder)
	Entity Type	Provider of drinking water services.
Structure of responsibility		<ul style="list-style-type: none"> <li>DuCoop (and its employees): granted access to the gathered data, but not held responsible for technical protection of that data.</li> <li>OpenMotics: data storage, data treatment.</li> <li>Farys: responsible for the IT solutions implemented at the pilot site, as well as the firewall protecting the local network.</li> </ul>
2.3	Rules and procedure	
Meetings	A meeting regarding data and data policies will be held every year, with the first one having taken place on December 8, 2020.	
Nomination	The employees of OpenMotics/DuCoop/Farys that are most relevant to security issues will convene during the governance body meetings.	
Publication of minutes	To be specified.	
2.4	Continual improvement and periodic update	
Meetings	A meeting regarding data and data policies will be held every year, with the first one having taken place on December 8, 2020.	
Evaluation procedure	An evaluation can take place after the 3rd workshop (where security and privacy analysis is carried out).	

3	DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data		DuCoop/OpenMotics
PII Controller		DuCoop
PII Processors		DuCoop/OpenMotics
PII Principals		Residents/building users
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		DuCoop and OpenMotics have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site (including data obtained in the context of InterConnect). The residents/building users that are the producers of data have all signed an informed consent form, confirming that their personal data can be used for research (not limited to InterConnect).

Agreement 1	Organizations	DuCoop & OpenMotics
	Agreement template	The agreement between DuCoop and OpenMotics is separate from the InterConnect project itself but covers all the required data management processes relevant to InterConnect.
3.2.2	Data description	
Data	Dates for collection	Starting date depends on when an asset is taken into operation and when communication infrastructure is in place. Data gathering for the different types of data currently obtained started between April 2020 and December 2020.
	Identification of data	<ol style="list-style-type: none"> <li>1. Electricity demand per living unit.</li> <li>2. Heat demand per living unit.</li> <li>3. Asset measurements (battery, heat pump, vacuum system, water treatment...).</li> <li>4. Measurements related to the district heating network (temperatures, pressures, flows...).</li> <li>5. Measurements related to the water treatment (vacuum system, ventilation, treatment...).</li> </ol>
	Type of data	<ol style="list-style-type: none"> <li>1. PII/critical to service data.</li> <li>2. PII/critical to service data.</li> <li>3. Critical to service data.</li> <li>4. Critical to service data.</li> <li>5. Critical to service data.</li> </ol>
	Life Cycle	According to the informed consent form (see Agreement approach), data obtained can be used for research purposes also beyond InterConnect. Historical data is also used to provide better services. No storage time/deletion process is therefore fixed at this point.
	Data description	To be specified.
3.2.3	Data exchange	
Data flow		<p>Based on <a href="https://www.linddun.org/linddun">https://www.linddun.org/linddun</a></p> <pre> sequenceDiagram     participant EU as Energy user     participant A as Assets     participant PLC     participant G as Gateway     participant DB as Database     participant S as Software platform provider/EMS     participant ESP as Energy service provider      EU-&gt;&gt;A: Deliver energy     A-&gt;&gt;PLC: Data transfer over PLC     A-&gt;&gt;G: Direct data transfer     G-&gt;&gt;DB: Data storage     DB-&gt;&gt;S: Data querying     S-&gt;&gt;S: Save EMS states     S-&gt;&gt;ESP: Calculate optimal Asset operation     ESP-&gt;&gt;S: Provide operational constraints     S-&gt;&gt;G: Send control signals     G-&gt;&gt;PLC:      PLC-&gt;&gt;A:      </pre> <p><b>FIGURE 21: DATA FLOW DIAGRAM NIEUWE DOKKEN GENT PILOT</b></p>





3.2.4	Data access monitoring
Data access verification procedure	To be specified.
3.2.5	Data Registry
Registry of agreements	To be specified.
Registry of data sets	To be specified.
Registry of citizen consents	To be specified.

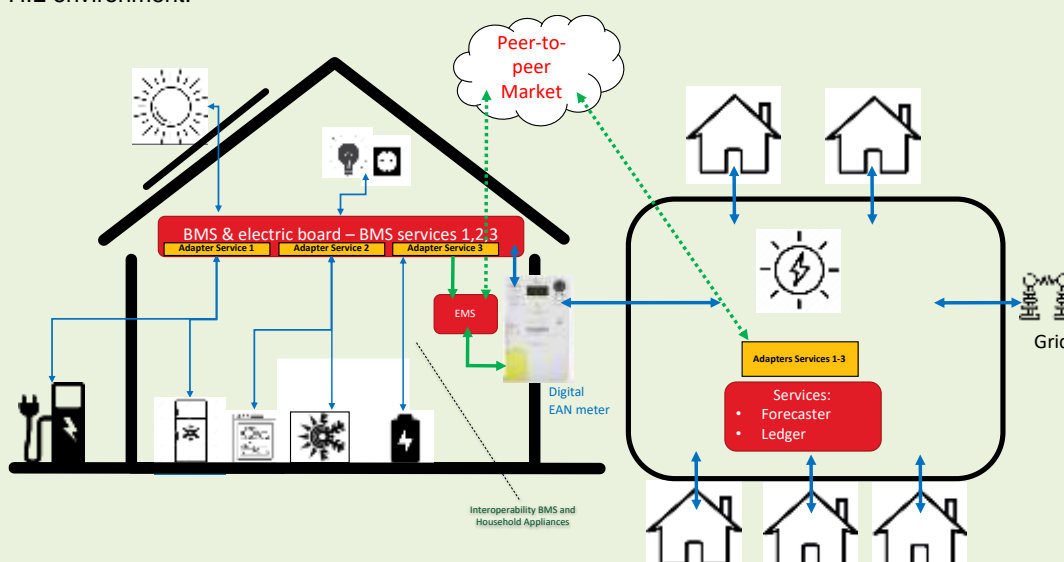
4	<b>RISK MANAGEMENT PLAN</b>	
4.1	Pilot needs and resources for security and privacy risk management	
Context for privacy analysis	Since part of the data obtained in the pilot will be used for invoicing, and thus directly impact natural persons, a privacy analysis is required.	
Context for security analysis	To be specified.	
Context for the project	To be specified.	
4.2	Risk management process	
4.2.1	Security	
Methodology	STRIDE Methodology	
Schedule	2nd Workshop in May/June	
Template	Use the InterConnect template.	
4.2.2	Privacy	
Methodology	LINDDUN Methodology	
Schedule	2nd Workshop in May/June	
Template	Use the InterConnect template.	

5	<b>ENGINEERING MANAGEMENT PLAN</b>	
Pilot needs and resources for security and privacy engineering	Interoperability framework: configurable access control Decision on some level of compliance per pilot. Current security and privacy capabilities include technical measures, encryption techniques and pseudonymisation techniques.	

Engineering process	NIST Methodology
Schedule	To be specified.

6	CITIZEN MANAGEMENT PLAN
Pilot needs and resources for management	DuCoop (operator of the pilot assets) has since the initiation of the pilot been in close contact with the pilot inhabitants, amongst others by personal contact and newsletters. Citizen interaction is therefore expected to run smoothly.
Management process	In their contract with DuCoop (see also Data Management Plan - Agreement Approach), pilot inhabitants are made aware of how their personal data can/will be used, and of how they can access and request adjustment of their data (i.e., by sending an email to a general DuCoop email address). Other than that, no specific actions were taken to make citizens aware of any possible data security issues.
Schedule	To be specified.

## ANNEX 2.1.6 ZELLIK GREEN ENERGY PARK BRUSSELS (VUB)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	ZELLIK GREEN ENERGY PARK BRUSSELS
SUMMARY	<p><b>Scope and objectives:</b></p> <ul style="list-style-type: none"> <li>The site mimics the behaviour of 6 households with complementary assets and user profiles in a full P2P energy trading market, without intermediaries in a real-life like environment. It aims to investigate the financial feasibility of such as system, the technological feasibility of the peer-to-peer supporting platform, and the impact on the self-consumption of locally produced energy.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p>The Green Energy Park will deploy the smart village lab during Q2 and Q3 2021. This will contain a building with 6 virtual dwellings, meaning 6 separate units that each have their own energy management system and building management system. The BMS's will control a different set of assets implemented in each of the dwelling units. This will encompass household appliances, charging posts, solar panels, heat pumps and home batteries. Unavailable appliances are emulated through a programmable load. As such, a wide variety of household configurations can be emulated through a HIL environment.</p>  <p><b>FIGURE 23: OVERVIEW ARCHITECTURE OF ZELLIK GREEN ENERGY PARK PILOT</b></p> <p>As shown in the graphic, the assets are controlled by a BMS system per unit, that is advised by a HEMS that measures production and consumption of the assets. The set up aims to implement 6 different EMS systems as well as 6 different BMS systems. The HEMS will communicate to other EMS by means</p>

	<p>of an interoperability platform sustained by an AZURE cloud. In addition, the HEMS will have access to several services such as market, production, and consumption forecasters, and will be able to optimally manage the energy of its dwelling unit and propose flexibility to the other households. At any time, each of the units can buy and sell energy its own supplier. Transactions will be supported by P2P marketplace. The set-up will allow to mimic the behaviour of essentially different users (singles, small and large families) with varying user preferences and habits. Several price settings for selling and buying will be experimented and the effect on LCOE, local RES consumption and peak shaving will be assessed, while the operational decisions with respect to the peer-to-trading are taken in distributed way. Emulated profiles for consumption and production are based on real-life measurements monitored on other sites and at private dwellings. The DSO is integrated as a hypothetical trader of distribution tariffs, hence contributing to peak shaving towards the grid. As such financial feasibility will be assessed for different configurations of energy communities, as well as the capability of the InterConnect solutions in supporting a peer-to-peer market.</p>
--	--

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		GDPR
International Standards		N/A
2.1 GOVERNANCE BODY		
Information Security Manager		Thierry Coosemans/Jimmy Van Moer (GEP vzw)
Data Protection Officer		Thierry Coosemans
Other roles		N/A
Ecosystem consideration		Governance of the site is carried out by Green Energy Park VZW.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	VUB (Vrije Universiteit Brussels)
	Role	Data Controller and energy manager
	Address	Pleinlaan 2, 1050 Brussels, Belgium
	Contact(s)	Thierry Coosemans: <a href="mailto:Thierry.Coosemans@vub.be">Thierry.Coosemans@vub.be</a>
	Entity Type	University
Entity 2	Entity Name	Green Energy Park VZW
	Role	Market supervisor
	Address	Zone1 Research Park 160/Z1, 1731 Asse, Belgium
	Contact(s)	Jimmy Van Moer: <a href="mailto:jimmy.vanmoer@greenenergypark.be">jimmy.vanmoer@greenenergypark.be</a>
	Entity Type	Research Infrastructure provider
Entity 3	Entity Name	Fluvius
	Role	Measurements
	Address	Brusselsesteenweg 199, 9090 Melle, Belgium
	Contact(s)	To be specified.
	Entity Type	DSO
Structure of responsibility		<ul style="list-style-type: none"> <li>VUB: carrying out research</li> <li>GEP VZW: responsible for installation, control, and maintenance infrastructure (hardware, data platform)</li> <li>Fluvius: DSO: providing measurements EAN, provides and maintains main substation at common point of coupling</li> </ul>
2.3 Rules and procedure		
Meetings		<ul style="list-style-type: none"> <li>Frequent meetings VUB- GEP for project implementation (as many as needed)</li> <li>Frequent meetings GEP with technology suppliers (as many as needed)</li> </ul>

Nomination	Researchers and personnel of VUB Personnel Green Energy Park vzw
Publication of minutes	To be specified.
2.4	Continual improvement and periodic update
Meetings	To be specified.
Evaluation procedure	An evaluation can take place after the 3rd workshop (where security and privacy analysis are carried out).

<b>3 DATA MANAGEMENT PLAN</b>		
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	Green energy park VZW, Vub	
PII Controller	There is no personal identifiable information, these are virtual based on anonymized profiles.	
PII Processors	There is no personal identifiable information, these are virtual based on anonymized profiles.	
PII Principals	There is no personal identifiable information, these are virtual based on anonymized profiles.	
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach	VUB and GEP VZW have access to data, since no personal data are used, no particular agreement is needed.	
Agreement 1	Organizations	N/A
	Agreement template	N/A
3.2.2	Data description	
Data	Dates for collection	Starting Q3 2021
	Identification of data	1. Consumption and production profiles housing units (energy, power, voltage, current), measured and forecasted data. 2. Synthetic user preferences. 3. Market prices energy.
	Type of data	1. Critical to service data. 2. Synthetic PII/ Critical to service data. 3. Business data.
	Life Cycle	1. Starting date: Q3 2021. 2. Storage time: at least duration of project. 3. Deletion process: no deletion process.
	Data description	1. Timeseries data: power, energy, voltage, current as a function of time. 2. Euro/kWH 3. Euro/kW
3.2.3	Data exchange	
Data flow	<ul style="list-style-type: none"> <li>Fluvius measures and conveys to GEP.</li> <li>GEP collects all measurements of all assets and conveys to VUB.</li> <li>VUB conveys setting parameters for market to GEP.</li> </ul>	
Data access control chart	To be specified.	
3.2.4	Data access monitoring	

Data access verification procedure	Limited persons have access to data; these are the researchers of the VUB and the operators of the Smart Village Lab. In addition, the DSO Fluvius has access to the EAN meters.
3.2.5	Data Registry
Registry of agreements	To be specified.
Registry of data sets	To be specified.
Registry of citizen consents	To be specified.

4	Risk Management Plan
4.1	Pilot needs and resources for security and privacy risk management
Context for privacy analysis	N/A
Context for security analysis	To be specified.
Context for the project	To be specified.
4.2	Risk management process
4.2.1	Security
Methodology	Market platform will be supported by Azure, with related security settings.
Schedule	2nd workshop around mid-June 2021.
Template	Use the InterConnect template.
4.2.2	Privacy
Methodology	N/A
Schedule	N/A
Template	N/A

5	Engineering Management Plan
Pilot needs and resources for security and privacy engineering	To be specified in 2021.
Engineering process	To be specified in 2021.
Schedule	Hardware will be installed during 2021 with basic functionality. Implementation will depend on readiness other WPs.

## 6 CITIZEN ENGAGEMENT PLAN

Not applicable to this pilot.

### ANNEX 2.1.7 OUD-HEVERLEE PUBLIC BUILDINGS (3E)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	OUD-HEVERLEE PUBLIC BUILDINGS
SUMMARY	<p><b>Scope and Objective:</b></p> <ul style="list-style-type: none"> <li>“Smartifying” my Local Energy Community.</li> </ul>

- In this use case end-users install the IoT solution for “smartifying” its thermal loads (water heaters, space heaters and heat pumps) to have controllability of them. This control capability is leveraged with the LEC as they can save money with aggregated peak shaving and self-consumption as well as flexibility provision.

NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.

#### DESCRIPTION

The objective of the pilot is to steer the HVAC system, EV charger and battery of a set of non-residential buildings to optimize the energy cost and limit the impact on the LV grid.

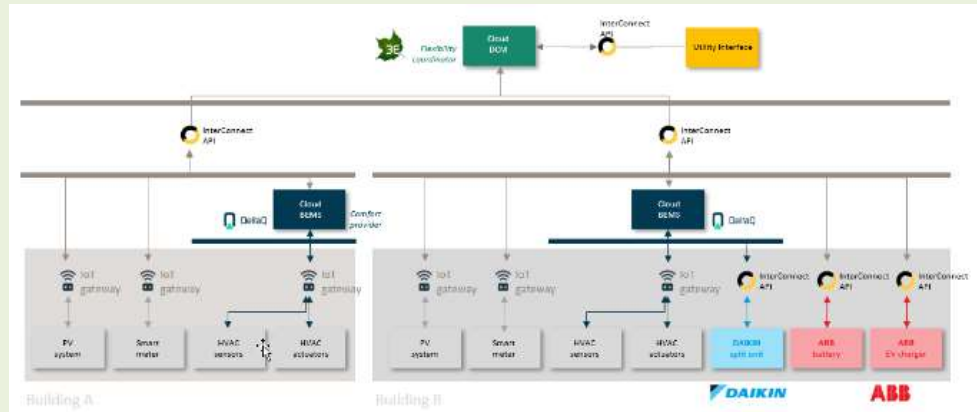


FIGURE 24: OVERVIEW ARCHITECTURE OF OUD-HEVERLEE PUBLIC BUILDINGS PILOT

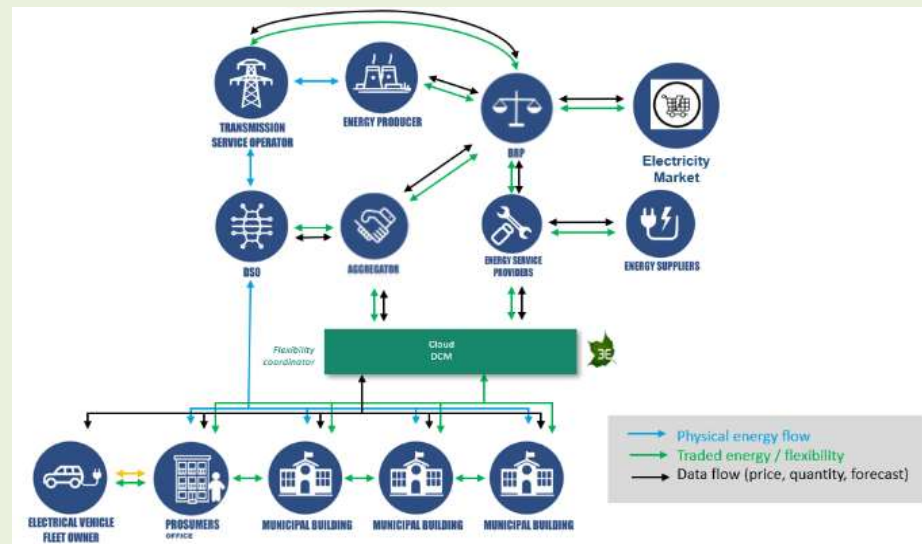


FIGURE 25: DIAGRAM OF DATA FLUX OF OUD-HEVERLEE PILOT

Energy community consists out of 4 buildings of the community (the city hall, OCMW office, police station and a day care centre) located next to each other in Oud-Heverlee pilot site. Necessary devices are as below:

- Hardware: new installations consist of:
  - A Daikin split-unit.
  - A battery of ABB.
  - An EV charger of ABB.
- Software: Generally, the HVAC installation of the building is controlled by a different software platform than the community demand management and grid interaction platform. On top of that, the battery or EV charger might be linked to proprietary software on cloud.
  - 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 is being extended to include the monitoring & control of batteries and EV chargers.
  - DeltaQ based on a model-predictive control framework automatically optimizes the BEMS control settings on hourly basis combining monitoring data, user preferences, weather forecasts and energy tariffs.
- Communication, monitoring and Control: IoT gateways, field sensors and actuators, smart meters, for power, heat, and comfort.

Steps are taken as below via interaction of different devices/actors:



	<ul style="list-style-type: none"> <li>Gathering measurements from the field sensor via field automation gateways into the laaS.</li> <li>Providing secure data I/O, account manager and User access via PaaS.</li> <li>Polling historical and current relevant measurements for forecasting.</li> <li>Establishing optimization model using forecasts via interaction with the User and the Utility interface manager.</li> <li>Multi-energy use optimization in a hierarchical distributed fashion.</li> <li>Traffic Light Control for setpoint/command deployment.</li> <li>Dashboard update.</li> </ul>
--	---

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		GDPR
International Standards		N/A
2.1 GOVERNANCE BODY		
Information Security Manager		Mojtaba Eliassi (3E)
Data Protection Officer		Mojtaba Eliassi (3E)
Other roles		N/A
Ecosystem consideration		No, i.e., the governance body might change after the InterConnect project.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	3E SynaptiQ
	Role	Community EMS
	Address	Quai à la Chaux 6, 1000 Bruxelles
	Contact(s)	Ruben Baetens (3E) < <a href="mailto:Ruben.Baetens@3e.eu">Ruben.Baetens@3e.eu</a> > Mojtaba Eliassi (3E) < <a href="mailto:MEL@3e.eu">MEL@3e.eu</a> > Julien Decks < <a href="mailto:JUD@3e.eu">JUD@3e.eu</a> >
	Entity Type	Community EMS provider
Entity 2	Entity Name	DeltaQ
	Role	HVAC EMS
	Address	Boulevard d'Anvers 40, 1000 Bruxelles
	Contact(s)	Benjamin De Dycker < <a href="mailto:Benjamin.DeDycker@deltaq.io">Benjamin.DeDycker@deltaq.io</a> > Jules Hammenecker < <a href="mailto:Jules.Hammenecker@deltaq.io">Jules.Hammenecker@deltaq.io</a> >
	Entity Type	HVAC EMS provider
Entity 3	Entity Name	CyberGrid
	Role	Flexibility Aggregator
	Address	Impulszentrum Lebring Parkring 6 8403 Lebring Austria
	Contact(s)	Cami Dodge-Lamm < <a href="mailto:camidodge@cyber-grid.com">camidodge@cyber-grid.com</a> > Andraž Andolšek < <a href="mailto:andraz.andolsek@cyber-grid.com">andraz.andolsek@cyber-grid.com</a> >
	Entity Type	Aggregation and VPP platform provide
Entity 4	Entity Name	ABB
	Role	EV charging station and Battery provider
	Address	Zaventem Belgium
	Contact(s)	Wouter Van Rysselberghe < <a href="mailto:wouter.vanrysselberghe@be.abb.com">wouter.vanrysselberghe@be.abb.com</a> >
	Entity Type	Battery and EV charging station and API manager provider

Entity 5	Entity Name	DAIKIN Europe (TBA)
	Role	Split unit provider
	Address	To be provided.
	Contact(s)	Jo Vandale < <a href="mailto:vandale.j@daikineurope.com">vandale.j@daikineurope.com</a> >
	Entity Type	HVAC system provider and its API manager
Entity 6	Entity Name	Community manager in Oud-Heverlee
	Role	Setting/preferences
	Address	Gemeentestraat 2, 3054 Oud-Heverlee, Belgium.
	Contact(s)	Marc Gilis < <a href="mailto:marc.gilis@oud-heverlee.be">marc.gilis@oud-heverlee.be</a> > Heleen Lambrechts < <a href="mailto:heleen.lambrechts@oud-heverlee.be">heleen.lambrechts@oud-heverlee.be</a> > Bart Clerckx < <a href="mailto:bart.clerckx@oud-heverlee.be">bart.clerckx@oud-heverlee.be</a> >
	Entity Type	Public entity
Structure of responsibility		<ul style="list-style-type: none"> <li>3E SynaptiQ and DeltaQ (and its eligible employees): Data storage, data treatment, granted access to the gathered data</li> <li>EV charger, battery, and HVAC manufacturers: data storage, data treatment; granted access to the gathered data</li> </ul>
2.3	Rules and procedure	
Meetings		<p>Several online/on-site meetings have been held for coordination amongst different actors separately and jointly making decision on data needs and exchange. A meeting regarding data and consent sharing is needed to be held after installation of the devices, and before sharing the first amounts of data between the participants.</p> <p>Regular pilot meetings, intercompany meetings/checks, and meetings organised in consortium. In case of incidents specific meetings will be organized.</p>
Nomination		Participation defined from the pilot partners.
Publication of minutes		TBS
2.4	Presentations and defined tasks (via e-mail, in MS teams and stored on MS SharePoint/NextCloud).	
Meetings		The project pilot is subject to change. This will be handled after finalising the pilot selection with the owner.
Evaluation procedure		The project pilot is subject to change. This will be handled after finalising the pilot selection with the owner.

3		DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.			
3.1		Pilot needs and resources for security and privacy data management	
Ownership of data		3E SynaptiQ, DeltaQ;	
PII Controller		3E SynaptiQ, DeltaQ; ABB EV charger; CyberGrid, DAIKIN	
PII Processors		3E SynaptiQ, DeltaQ; ABB; DAIKIN; CyberGrid	
PII Principals		Community manager/Owners	
3.2		Data Management Process	
3.2.1		Agreements	
Agreement approach		The agreements are planned and will be done before the pilot starts.	
Agreement 1	Organizations	3E SynaptiQ, DeltaQ, The community manager/owners, CyberGrid	

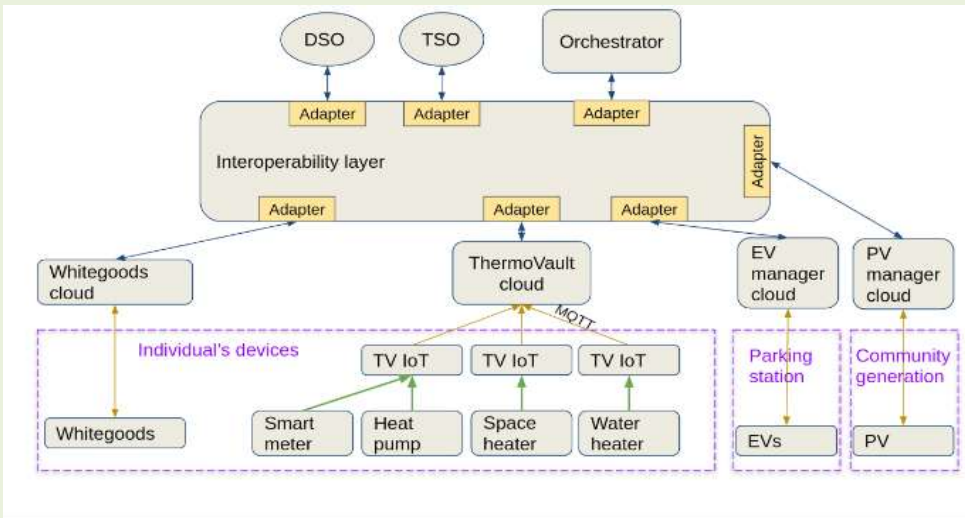
	Agreement template	As expressed before, the agreement template must be built as a phase of implementation.
3.2.2	Data description	
Data	Dates for collection	After complete installation of devices and field automation gateway. Historical metering data are currently being exchanged for proper sizing of EV charger, Battery, Split units, and PV for the buildings. Expected to be on last quarter of 2021.
	Identification of data	The service API inputs are: <ol style="list-style-type: none"> <li>1. On-site non-flexible load demand &amp; its forecast.</li> <li>2. On-site non-flexible load generation &amp; its forecast.</li> <li>3. On-site flexibility of devices in profile &amp; its forecast.</li> <li>4. Desired thermal comfort &amp; its forecast.</li> <li>5. Energy contracts of the community members.</li> <li>6. Local tariffs for grid use, energy use and injection (self-consumption scheme characteristics).</li> <li>7. Incentives for flexibility provision/Contract with the Aggregate: Commanded power or imposed price/incentives from the aggregator, retailer, or DSO.</li> </ol>
	Type of data	From 1 to 7: Critical to service data. From 5 to 7: Business data.
	Life Cycle	<i>To be specified.</i>
	Data description	As presented in identification of data. More details will be presented later.
3.2.3	Data exchange	
	Data flow	It will be updated when it is specified in the pilot.
	Data access control chart	It will be updated when it is specified in the pilot.
3.2.4	Data access monitoring	
	Data access verification procedure	Limited accessibility of data to an automatized body with granted access during design, implementation, and operation. Access of a third party should be granted having the consent of data owner and principal.
3.2.5	Data Registry	
	Registry of agreements	<i>To be specified.</i>
	Registry of data sets	<i>To be specified.</i>
	Registry of citizen consents	<i>To be specified.</i>

4	Risk Management Plan	
4.1	Pilot needs and resources for security and privacy risk management	
	Context for privacy analysis	<i>To be specified.</i>
	Context for security analysis	<i>To be specified.</i>
	Context for the project	<i>To be specified.</i>
4.2	Risk management process	
4.2.1	Security	
	Methodology	<i>To be specified.</i>
	Schedule	2nd workshop to be held on May/June 2021
	Template	InterConnect template for risk analysis will be provided and used to conduct the analysis.
4.2.2	Privacy	
	Methodology	<i>To be specified.</i>

Schedule	2nd workshop to be held on May/June 2021
Template	InterConnect template for the Privacy Impact Assessment will be provided and used to conduct the analysis.

6	Citizen Management Plan
Pilot needs and resources for management	For the installation and steering of EVs, Battery, and HVAC system, involvement of the manufacturer and its EMS is required. Interaction will be with the community manager to provide setting/preferences/confirmation.
Management process	The community member will be informed about the shared data and its purpose to confirm/reject data exchange. It will be presented to the community member the purposes of this data collection and conditions of sharing.
Schedule	Gateway will be installed during 2021 with basic SaaS functionality. Flexibility provision Implementation will depend on readiness other WPs.

## ANNEX 2.1.8 MECHELEN (THERMOVAULT)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	MECHELEN
SUMMARY	<p><b>Scope and Objectives:</b></p> <ul style="list-style-type: none"> <li>“Smartifying” my Local Energy Community: end-users install the IoT solution for “smartifying” its thermal loads (water heaters, space heaters and heat pumps) to have controllability of them. This control capability is leveraged with the LEC as they can save money with aggregated peak shaving and self-consumption.</li> <li>Energy flexibility service for spot prices electricity tariffs: end-user installs the IoT solution for “smartifying” its thermal loads (water heaters, space heaters and heat pumps) to have controllability of them. This control capability is used to decrease electricity bills by shifting consumption from expensive to cheap periods.</li> </ul> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	 <p><b>FIGURE 26: OVERVIEW ARCHITECTURE MECHELEN PILOT</b></p> <p>This pilot is set in a residential apartment building with 27 apartments. The idea is that the aggregator collects the consumption data and the forecasted household data and then optimize the loads for self-consumption, peak shaving, and dynamic pricing, based on SAREFized inputs from other interconnected actors. This is sent to the different appliances that also report their operation status to</p>

	the aggregator in real-time. This allows to adjust the consumptions and gives flexibility with the main goal to save energy and reduce energy bill.
--	---

<b>2 GOVERNANCE MANAGEMENT PLAN</b>		
Rules and legislation		GDPR
International Standards		N/A
<b>2.1 GOVERNANCE BODY</b>		
Information Security Manager		Pol Olivella
Data Protection Officer		Pol Olivella
Other roles		N/A
Ecosystem consideration		No, i.e., the governance body might change after the InterConnect project.
<b>2.2 ORGANISATION RESPONSIBILITY</b>		
Entity 1	Entity Name	ThermoVault
	Role	Data Controller
	Address	Hoefstadstraat 86, 3600 Genk, Belgium
	Contact(s)	Pol Olivella, <a href="mailto:olivella@thermovault.com">olivella@thermovault.com</a>
	Entity Type	Space and water heating hard- and software and EMS steering provider
Entity 2	Entity Name	Whitegoods manufacturers
	Role	Data Controller
	Address	-
	Contact(s)	<i>To be specified.</i>
	Entity Type	Appliance provider
Entity 3	Entity Name	Whitegoods EMS
	Role	Data Processor
	Address	-
	Contact(s)	<i>To be specified.</i>
	Entity Type	Provider of steering of whitegoods appliances
Structure of responsibility		<ul style="list-style-type: none"> <li>ThermoVault (and its eligible employees): data storage, data treatment, granted access to the gathered data.</li> <li>Whitegoods manufacturer: data storage, data treatment.</li> <li>EMS whitegoods: data treatment, granted access to the gathered data.</li> </ul>
<b>2.3 Rules and procedure</b>		
Meetings		A meeting regarding data and consent sharing will be held after installation of the devices, and before sharing the first amounts of data between the participants.
Nomination		<i>To be specified.</i>
Publication of minutes		<i>To be specified.</i>
<b>2.4 Continual improvement and periodic update</b>		
Meetings		<i>To be specified.</i>
Evaluation procedure		<i>To be specified.</i>

<b>3 DATA MANAGEMENT PLAN</b>		
InterConnect data management plan is the first input.		
<b>3.1 Pilot needs and resources for security and privacy data management</b>		
Ownership of data		ThermoVault /Whitegoods manufacturer / Whitegoods EMS provider
PII Controller		ThermoVault /Whitegoods manufacturer
PII Processors		Whitegoods EMS provider
PII Principals		Residents/building users
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach		ThermoVault and the tenants have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site. The residents/building users that are the producers of data have all signed an informed consent form, which needs to be extended specifically to the InterConnect project. In addition, a data processing agreement with the Whitegoods AMS provider will need to be made in the informed consent form.
Agreement	Organizations	ThermoVault /Whitegoods manufacturer / Whitegoods EMS provider
	Agreement template	A contract between the parties ThermoVault, Whitegoods manufacturer and Whitegoods EMS provider will need to be made.
<b>3.2.2 Data description</b>		
Data	Dates for collection	Expected in the last quarter of 2021 start of data collection and sharing.
	Identification of data	Electricity demand per living unit. Water and space heating electricity demand per living unit. Room and water vessel temperature measurements.
	Type of data	PII/critical to service data. PII/critical to service data. PII/critical to service data.
	Life Cycle	To be specified.
	Data description	The data Q4 2021 - end of project. Q4 2021 - end of project. Q4 2021 - end of project.
<b>3.2.3 Data exchange</b>		
Data flow		<i>To be specified.</i>
Data access control chart		<i>To be specified.</i>
<b>3.2.4 Data access monitoring</b>		
Data access verification procedure		<i>To be specified.</i>
<b>3.2.5 Data Registry</b>		
Registry of agreements		<i>To be specified.</i>
Registry of data sets		<i>To be specified.</i>
Registry of citizen consents		<i>To be specified.</i>



<b>4</b>	<b>Risk Management Plan</b>
<b>4.1</b>	<b>Pilot needs and resources for security and privacy risk management</b>
Context for privacy analysis	DPIA threshold is exceeded due to the amount, nature, and quantity of data gathered, necessitating a privacy analysis.
Context for security analysis	<i>To be specified.</i>
Context for the project	<i>To be specified.</i>
<b>4.2</b>	<b>Risk management process</b>
<b>4.2.1</b>	<b>Security</b>
Methodology	<i>To be specified.</i>
Schedule	2nd workshop to be held on May/June 2021
Template	InterConnect template for risk analysis will be provided and used to conduct the analysis.
<b>4.2.2</b>	<b>Privacy</b>
Methodology	CNIL
Schedule	2nd workshop to be held on May/June 2021.
Template	InterConnect template for the Privacy Impact Assessment will be provided and used to conduct the analysis.

<b>5</b>	<b>Engineering Management Plan</b>
Pilot needs and resources for security and privacy engineering	Current security and privacy capabilities include technical measures and encryption techniques.
Engineering process	<i>To be specified.</i>
Schedule	<i>To be specified.</i>

<b>6</b>	<b>Citizen Management Plan</b>
Pilot needs and resources for management	ThermoVault is in close interaction with the pilot participants for their heating needs. For the installation and steering of whitegoods, involvement of the manufacturer and/or EMS steering provider is expected.
Management process	Pilot participants are clearly informed in the consent on form on the amount and nature of shared data, as well as their purpose.
Schedule	<i>To be specified.</i>

## ANNEX 2.2 GREEK PILOT SPP

<b>1</b>	<b>SECURITY AND PRIVACY PLAN CONTEXT</b>
PILOT NAME	GREEK PILOT
SUMMARY	<p><b><u>Scope and objectives:</u></b></p> <ul style="list-style-type: none"> <li>• This pilot is focused on 9 different use cases to save energy and flexibility services:</li> <li>• Energy Monitoring &amp; Management</li> <li>• Home Comfort</li> <li>• Flexibility Provision</li> <li>• Data analytics Services</li> <li>• Security services</li> </ul>

- Increase CO2 savings and become eco-friendly
- User Engagement
- Unified User Interface Application
- Appliances' energy efficiency

NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.

## DESCRIPTION

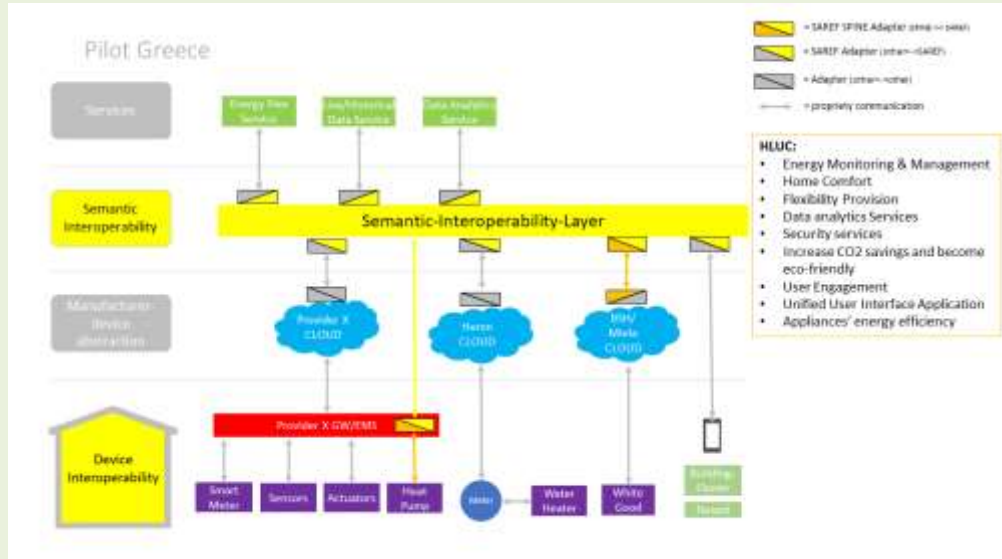


FIGURE 27: OVERVIEW ARCHITECTURE OF GREEK PILOT

### Energy monitoring and 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.

### 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.

### 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 1) monitor the current state of their home appliances; 2) one day-ahead decide when they will participate in a demand response scheme (opt-in/out for the next 24 hours); 3) one day-ahead configure which appliances will be part of their harnessed flexibility that will be released in the system.

To achieve the aforementioned goal, their consumption data should be collected by various installed smart meters/plugs 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, decide on 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.

### 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, producers/operators can provide tailored-made offers based on their customers' needs and give them bonuses/incentives for shifting loads to off-peak hours.

#### **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.

#### **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.

#### **User engagement:**

- Education
  - Educate customers through energy tips and enable them to be more energy efficient and reduce their electricity bill. GRID operators will educate their customers through a user interface by providing them with energy efficiency tips and recommendations. Consumers on their end will increase their awareness around energy efficiency and in the end, they will achieve lower energy bills.
- Gamification
  - This Use Case describes how to pay less through gamification challenges. GRID operators will provide challenges and personal targets through a mobile app developed by a technology provider. Consumers will earn rewards in terms of energy points and ranking among other consumers. In the end, consumers will see their electricity bills reduced by accomplishing the challenges and targets in the context of gamification.
- Loyalty Program
  - This Use Case describes how to pay less through benefits redeemed for the consumers' actions. GRID operators will engage in B2B agreements with 3rd parties so that consumers will be able to redeem energy points in various businesses (Shopping, Tickets, Gadgets, etc.). Consumers earn energy points for responding to GRID's demand for actions (load shifting, increase/decrease consumption) that are made through a mobile app (developed by a technology provider).

#### **Unified user interface application:**

By means of state-of-the-art technologies and secure interfaces, the end user will be 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.

#### **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.
--	---

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation		Rules defined in the Grant Agreement of the project apply in this pilot. GDPR rules apply since we are dealing with Personally identifiable information from home IoT devices like sensors and energy consumption monitoring from smart meters. Consumers provide their consent on the processing of their anonymized data by 3rd parties to be offered with services and be part of the pilot demonstrations.
International Standards		N/A
2.1 GOVERNANCE BODY		
Information Security Manager		Donatos Stavropoulos: <a href="mailto:ds@gridnet.gr">ds@gridnet.gr</a> (GRIDNET)
Data Protection Officer		Donatos Stavropoulos: <a href="mailto:ds@gridnet.gr">ds@gridnet.gr</a> (GRIDNET)
Other roles		N/A
Ecosystem consideration		N/A
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	GRIDNET S.A.
	Role	Technology Provider (Provide anonymized energy data out of user premises)
	Address	Riga Feraiou 119, Volos 38221, Greece
	Contact(s)	Donatos Stavropoulos : ( <a href="mailto:ds@gridnet.gr">ds@gridnet.gr</a> )
	Entity Type	SME - Technology Provider
Entity 2	Entity Name	COSMOTE
	Role	Technology Provider (Provide anonymized energy data out of user premises)
	Address	Leof. Kifisias 99, Marousi 15124, Athens, Greece
	Contact(s)	George Lyberopoulos : ( <a href="mailto:glimperop@cosmote.gr">glimperop@cosmote.gr</a> )
	Entity Type	Telecom operator - Technology Provider
Entity 3	Entity Name	HERON
	Role	Electricity generator – Supplier (Provide anonymized energy data out of user premises)
	Address	124 Av. Kifissias & Iatridou, Athens 11526, Greece
	Contact(s)	Konstantina Montesidi : ( <a href="mailto:kmedesidi@heron.gr">kmedesidi@heron.gr</a> ), Dimitris Chatzigiannis : ( <a href="mailto:dchatzigiannis@heron.gr">dchatzigiannis@heron.gr</a> ), Andreas Sakellaropoulos : ( <a href="mailto:asakellaropoulos@heron.gr">asakellaropoulos@heron.gr</a> )
	Entity Type	SME – Data Provider
Entity 4	Entity Name	WINGS
	Role	ICT supplier (Process anonymized energy data for data analytics purposes)
	Address	189, Syggrou Avenue, 17121 Athens, Greece
	Contact(s)	Tilemachos Doukoglou, Andreas Georgakopoulos, Grigoris Maragkakis, Aspa Skalidi, Panagiotis Vlachas, Vassilis Foteinos, Panagiotis Demestichas {tdoukoglou, andgeorg, gmaragkakis, askalidi, panvlah, vfotein, pdemest}@wings-ict-solutions.eu
	Entity Type	SME

Entity 5	Entity Name	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER (AUEB-RC)
	Role	Technology Provider, Research organization (Process anonymized energy data for consumer engagement purposes through a mobile app system)
	Address	Kefallinias Street 46, 11251, Athens, Greece
	Contact(s)	George C. Polyzos, Iordanis Koutsopoulos, Vasilios A. Siris, Spiros Chadoulos {polyzos, jordan, vsiris, spirosch}@aueb.gr
	Entity Type	Academic Institution, Research organization
Entity 6	Entity Name	Inetum Realdolmen BE
	Role	ICT supplier (Provide Demand-Response solution)
	Address	Albert Vaucampslaan 42 1654 Huizingen Belgium
	Contact(s)	María Pérez Ortega
	Entity Type	Global ICT provider
Structure of responsibility		The structure of responsibility between organization for security and privacy purposes is formed by the rules of the Grant Agreement.
2.3	Rules and procedure	
Meetings		Regular Pilot meetings (monthly) and General Assembly meetings (yearly).
Nomination		Agreement among the responsible entities.
Publication of minutes		Minutes and presentations available after the meetings to the consortium of the project.
2.4	Continual improvement and periodic update	
Meetings		The meetings are called on demand in case of an incident or a proposal for improvement by a responsible entity.
Evaluation procedure		Evaluation will take place after the 3rd workshop (where security and privacy analysis are carried out)

3	DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
GRIDNET' s Households Dataset	Ownership of data	Consumers & GRIDNET
	PII Controller	GRIDNET
	PII Processors	N/A
	PII Principals	Consumers
COSMOTE' s Households Dataset	Ownership of data	Consumers & COSMOTE
	PII Controller	COSMOTE
	PII Processors	N/A
	PII Principals	Consumers
HERON' s Households Dataset	Ownership of data	Consumers & HERON
	PII Controller	HERON
	PII Processors	N/A
	PII Principals	Consumers
3.2	Data Management Process	
3.2.1	Agreements	

Agreement approach		The PII Controller with the consent of the PII Principal anonymizes the dataset from the smart-meter and the dataset from the sensors of the house (if any) before providing it to 3rd parties for processing. An agreement between the PII Controller and a 3rd party that acts as a Data Processor dictates the terms under which the data sharing between these two entities takes place.
Agreement 1	Organizations	GRIDNET, COSMOTE, HERON as Data Suppliers WINGS, AUEB, GFI as Data Processors
	Agreement template	Agreement: <ul style="list-style-type: none"> <li>Grant Agreement</li> <li>Terms and Conditions for Data Access (Agreement between data suppliers and data processors)</li> </ul>
3.2.2 Data description		
GRIDNET's Households Dataset	Dates for collection	1/10/2019 – 30/11/2023
	Identification of data	Energy data: <ul style="list-style-type: none"> <li>Whole home energy consumption (smart meter).</li> <li>Appliance/Device energy consumption.</li> </ul> Sensor data: <ul style="list-style-type: none"> <li>Temperature/Humidity indoor and outdoor</li> <li>Door/window contact</li> <li>Motion</li> <li>Illuminance</li> </ul>
	Type of data	Household data related to energy consumption and home environment.
	Life Cycle	<ul style="list-style-type: none"> <li>Energy data is generated every 17 seconds.</li> <li>Sensor data is generated on sensors' status change.</li> <li>Data is stored in the cloud without any expiration/deletion date.</li> </ul>
	Data description	Measurements Section: <a href="https://homegrid.gridnet.gr/Documentation/#measurements">https://homegrid.gridnet.gr/Documentation/#measurements</a>
COSMOTE's Households Dataset	Dates for collection	05/10/2019 - 30/11/2023
	Identification of data	Energy Data <ul style="list-style-type: none"> <li>Total and per phase power and energy consumption (smart meter)   Voltage and current related measurements are also available.</li> <li>Appliance/Device power/energy consumption.</li> </ul> Sensors Data <ul style="list-style-type: none"> <li>Temperature/Humidity/Pressure (indoor, outdoor).</li> <li>Door/Window contact sensor status (open, close).</li> <li>Smart plug / lights switch status (on, off).</li> <li>Motion / Activity (PIR sensor, IP camera).</li> <li>Luminance.</li> <li>Fire /Gas /Carbon Monoxide/Dioxide.</li> <li>Alarm (on, off).</li> <li>Physical Buttons and Virtual Switches status (on, off, single-click, double-click).</li> </ul> Actuation-related commands and alerting, based on smart plugs / lights switches (on, off), IR hubs, alerts based on rules/events, etc.
	Type of data	Household data related to power/energy consumption, home comfort and security.
	Life Cycle	Power/Energy Data is generated every 15 seconds. This interval may be customised depending on the needs of the pilot.  Sensor Data is generated based on sensors' status change (see Window/door or PIR sensor) and/or upon specific time intervals determined by the sensor itself, the access technology it employs (ZigBee, z-wave, Wi-Fi), whether it is battery powered or not, etc. Customized time intervals can be achieved using custom sensors; could be made available.  Data is stored in cloud infrastructure without any expiration/deletion date.

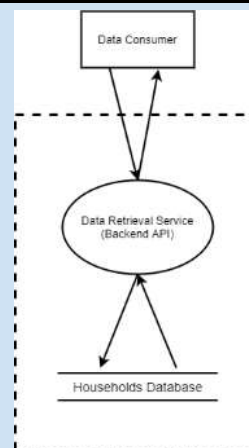


	Data description	Energy Data: IC Regular Services Survey Response - LeonR&Do Energy Monitoring Service [ <a href="#">Link</a> ] Home Comfort Data: IC Regular Services Survey Response - LeonR&Do Home Comfort Monitoring [ <a href="#">Link</a> ]
HERON' s Households Dataset	Dates for collection	1/8/2020-starting date of collection of real-time energy measurements for the project purposes. End: 30/11/2023
	Identification of data	Energy data Total home energy consumption (readings from smart meters).
	Type of data	Real-time measurements of electricity consumption.
	Life Cycle	Data logging is of 5-min for energy and 30 sec for the rest measured parameters. The collected data is anonymized prior sharing with the other project partners without any expiration/deletion date. This anonymized consumption data is stored in a cloud provider, whose servers are in the European Union.
	Data description	Real-time series data available from smart meters recording the following measured parameters: <ul style="list-style-type: none"> <li>• Active power</li> <li>• Reactive power</li> <li>• Voltage</li> <li>• Energy</li> <li>• Power factor</li> </ul>

### 3.2.3

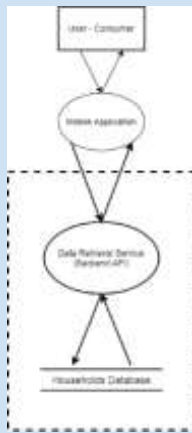
### Data exchange

#### Data flow



**FIGURE 28: DATA FLOW DIAGRAM GREEK PILOT**

Based on <https://www.linddun.org/linddun>

Data access control chart	 <p><b>FIGURE 29: DATA ACCESS DIAGRAM GREEK PILOT</b></p>
3.2.4	Data access monitoring
Data access verification procedure	Each Data Supplier provides/revokes access to data manually and explicitly to a Data Consumer/Processor.
3.2.5	Data Registry
Registry of agreements	<ul style="list-style-type: none"> <li>Project's drive (digital)</li> <li>Companies' headquarters (hard copies)</li> </ul>
Registry of data sets	<ul style="list-style-type: none"> <li>GRIDNET's Households Dataset is stored in company's private server.</li> <li>COSMOTE's Households Dataset is stored in company's private server.</li> <li>HERON's Households Dataset is stored in company's private server.</li> </ul>
Registry of citizen consents	<p>GRIDNET receives written consent regarding the free installation of the equipment in the house and the use of their anonymized measurements by 3rd parties in the context of the INTERCONNECT project.</p> <p>COSMOTE receives a written consent regarding the installation of equipment at the friendly-user house and the use of related measurements by 3rd parties in the context of the INTERCONNECT project.</p> <p>HERON initially informs its customers about the capability of participating in the company's research programs and consumers who express their interest in participating in the pilot will be invited to register online in the energy metering platform of HERON. The registration will be successfully accomplished only when the consumer has acknowledged that s/he has read the privacy notice and has accepted the relevant terms and conditions for participating along with the provision of his/her consent online at the time of registration to participate in the pilot.</p> <p>Consumers provide their consent by agreeing in terms and conditions before being able to use the mobile app developed for the Greek Pilot.</p>

4	<b>Risk Management Plan</b>
4.1	Pilot needs and resources for security and privacy risk management
Context for privacy analysis	<p>All the use cases in the pilot are using anonymized data from households. The data processors identify the different datasets by a home-id but they are not aware of the home's exact location (they can know the city) and the resident's personal information.</p> <p>The information that connects the home-ids with the location and the name of the resident is only known to the Data Suppliers who were also responsible for the hardware installation in the houses.</p>
Context for security analysis	<p>Even though the datasets are anonymized, they are not open and free. For that reason, access should be given only to entities/persons that have the task to implement the pilot's use cases. Data transfer should be encrypted from the home IoT device, through the cloud database to the Data Processor. Authentication/Authorization mechanisms should prevent any data breach in the database.</p>

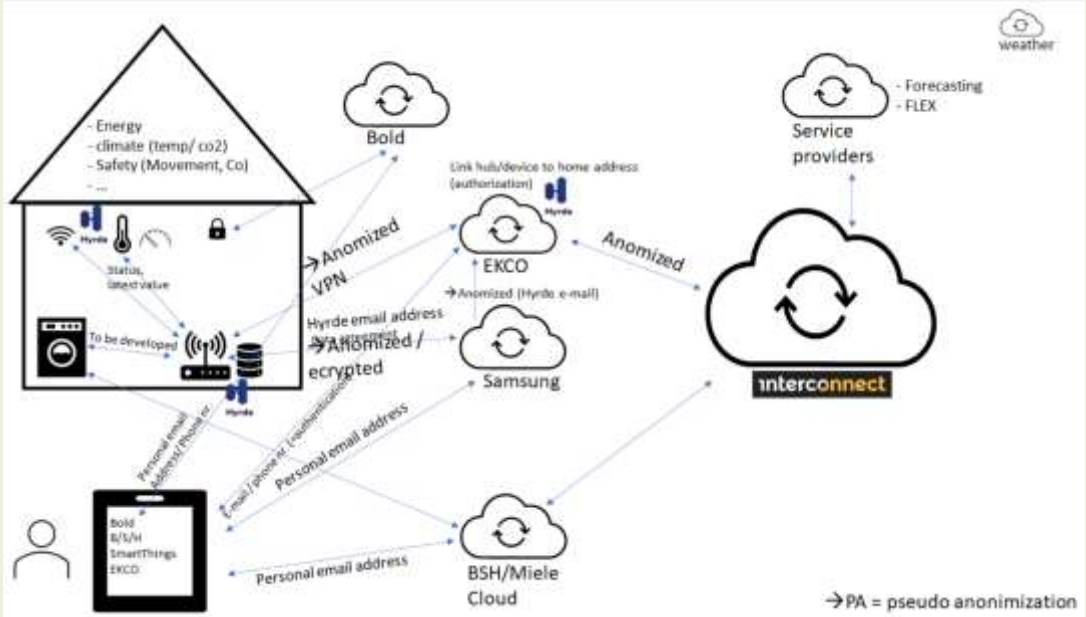
Context for the project	See above.
4.2	Risk management process
4.2.1	Security
Methodology	<p>STRIDE</p> <ul style="list-style-type: none"> <li>Security Properties: Authentication, Integrity, Non-Repudiation, Confidentiality, Availability, Authorization</li> <li>Security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege</li> </ul> <p>NIST Security Framework (e.g., Identify, Protect, Detect, Respond, and Recover).</p>
Schedule	2nd workshop to be held on May/June 2021
Template	InterConnect template for risk analysis will be provided and used to conduct the analysis.
4.2.2	Privacy
Methodology	<p>LINDDUN</p> <ul style="list-style-type: none"> <li>Privacy properties: unlinkability, Anonymity, Plausible deniability, Undetectability, Confidentiality, Context-Awareness, and Consent Compliant.</li> <li>Privacy Threats: Linkability, Identifiability, Non-Repudiation, Undetectability, Disclosure of Information, Context unawareness, Consent, Non-compliance.</li> </ul> <p>NIST Privacy Framework (identify, Govern, Control Communicate and Protect)</p>
Schedule	2nd workshop to be held on May/June 2021
Template	InterConnect template for the Privacy Impact Assessment will be provided and used to conduct the analysis.

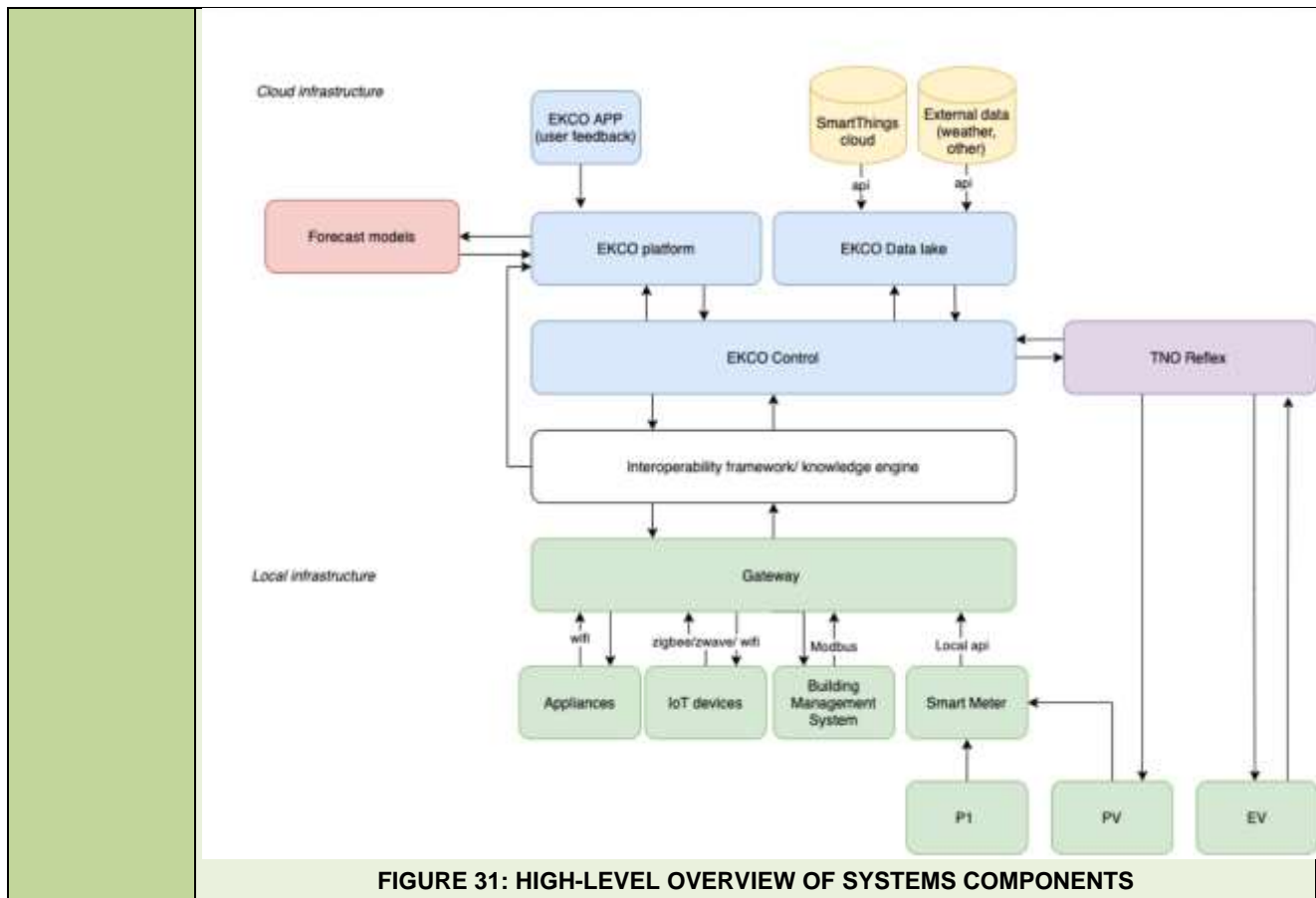
<b>5</b>	<b>Engineering Management Plan</b>
Pilot needs and resources for security and privacy engineering	Currently each Data Supplier implements its own access control mechanism, which complicates things for the Data Processors who need access to all the three Data Suppliers (GRIDNET, COSMOTE, HERON) to implement the pilot's use cases. Therefore, we will investigate the possibility of adopting the access control mechanism that will be provided by the Interoperability framework.
Engineering process	<p>Methodologies identified for the engineering process:</p> <ul style="list-style-type: none"> <li>NIST Frameworks (Security and Privacy)</li> <li>ISO/IEC 27550</li> <li>ISO/IEC 27001 and 27701</li> </ul>
Schedule	After the 2nd Workshop and before M24 (September 21)

<b>6</b>	<b>Citizen Management Plan</b>
Pilot needs and resources for management	<p>Users need to provide their consent to the Data Controllers.</p> <p>Users need to provide their consent to the Data Processors.</p>
Management process	<p>Data Controllers that are also responsible for the hardware installation of the various sensing devices in the house, receive the user's consent before the installation. Users can monitor their house environment and energy consumption, while Data Controllers are able to process their data and offer services to the users (dashboards, remote control/monitoring, etc.). Moreover, Data Controller can provide their data (anonymized) to 3rd parties to provide advanced services to the users as an exchange (data analytics, recommendations etc.).</p> <p>In the context of the pilot's use cases, users will be asked to use a mobile application developed by a Data Processor. Once the user opens the application, he will be informed about the usage of his/her data and provide his/her consent to proceed.</p>

Schedule	<p>Consent from the users regarding the Data Controllers will be given before M24 (Sept 21).</p> <p>Consent from the users regarding the mobile application and their data processing will be given at the time the user opens the application.</p>
----------	---

## ANNEX 2.3 DUTCH PILOT SPP

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	HLUC1 Smart buildings / Energy - Optimize sustainability
SUMMARY	<p><b>Scope and objectives:</b></p> <p>The objective of this pilot is to save energy by intelligent use and smart management of the building and its devices, derived from data driven services. For example: Lights on/off based on presence, ventilation based on occupation, adaptive heating/cooling based on weather and occupation, start on home appliance based on PV generation. By use of a battery reduce the peak load for EV charging and store and optimize RES from e.g., PV panels.</p> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p>The building owner reduces its energy costs and optimizes the use of RES.</p> <p>The building manager/facility manager can monitor (through a dashboard) and control the building installations (BMS).</p> <p>The facility manager can view the current usage and occupation of the building.</p> <p>The building owner has access to flexible tariffs and current energy schedules.</p> <p>The shared mobility company has access to three quick chargers and provides their charging needs.</p> <p>Simplified, a general overview diagram, see below:</p>  <p><b>FIGURE 30: GENERAL OVERVIEW DIAGRAM OF DUTCH PILOT</b></p> <p>Central monitoring and control of lights, ventilation, cooling, heating (including use preferences).</p> <p>Central monitoring of energy consumption and forecasting.</p> <p>Optimization of EV Charge Lounge (EV chargers and maximize RES).</p> <p>PV energy forecast for current and next day.</p> <p>Energy storage for peak load and RES optimization.</p> <p>Energy suppliers provides flexible tariffs on 15 minutes (PTU) basis.</p> <p>Systems like Ekco IoT platform, ReFlex, ...together with the InterConnect Framework perform this task.</p> <p>Systems like Ekco IoT platform, ReFlex, VU Forecaster and Ekco Control (EMS and BMS together) perform this task.</p>



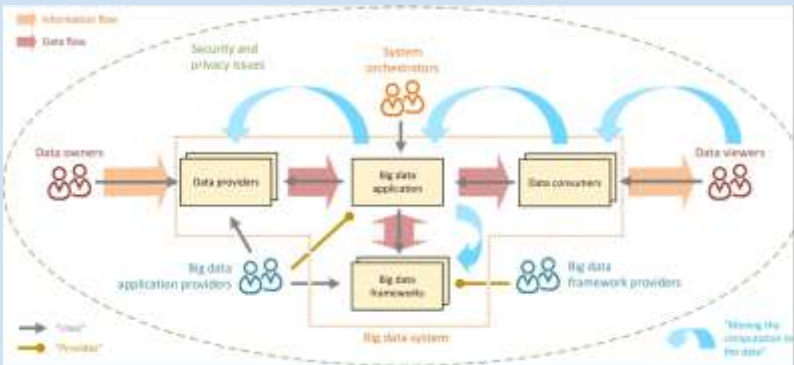
2		GOVERNANCE MANAGEMENT PLAN	
Rules and legislation		GDPR	
International Standards		CEN-CENELEC JTC13 - 27701 PIMS (extensions for GDPR) ENISA certification schemes for IoT	
2.1		GOVERNANCE BODY	
Information Manager	Security	Within the different involved organizations, the following persons are responsible for reporting on the performance of information security <ul style="list-style-type: none"><li>• Hyrde: Gert Kleijer</li><li>• TNO: Gjalt Loots,</li><li>• VU Amsterdam: Roderick van der Weerdt</li></ul> For the pilot this information will be centralised via VolkerWessels: Wouter Beelen and Mirjam Vaal	
Data Protection Officer		Within the different involved organizations, the following persons are responsible for reporting on the performance of information security <ul style="list-style-type: none"><li>• Hyrde: Gert Kleijer</li><li>• TNO: Remy v.d. Boom</li><li>• VU Amsterdam: The contact person will be Roderick van der Weerdt.</li></ul> There is a Data Protection Officer present at the VU, they can be contacted through: functionarisgegevensbescherming@vu.nl For the pilot this information will be centralised via VolkerWessels: Wouter Beelen and Mirjam Vaal	
Other roles		Depending on the structure TNO can participate with their DPO or their Project Manager in one of these bodies.	
Ecosystem consideration		To be specified.	

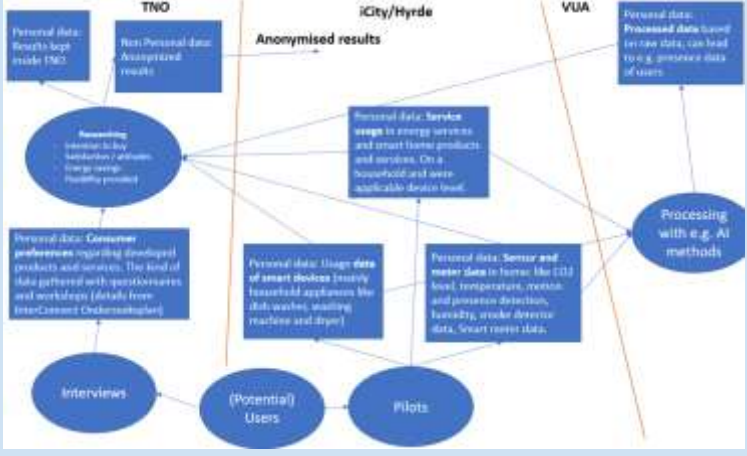

2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	VolkerWessels iCity
	Role	Pilot coordinator /governance
	Address	Torenallee 20, 5617 BC, Eindhoven, Nederland
	Contact(s)	Wouter Beelen: <a href="mailto:wbeelen@volkerwessels.com">wbeelen@volkerwessels.com</a>
	Entity Type	Private owned
Entity 2	Entity Name	Hyrde
	Role	Data processor
	Address	Modemweg 33, 3821 RS, Amersfoort, Nederland
	Contact(s)	Gert Kleijer
	Entity Type	Private owned
Entity 3	Entity Name	TNO
	Role	Data processor
	Address	Locatie Groningen. Eemsgolaan 3 9727 DW Groningen , Nederland
	Contact(s)	Gjalt Loots
	Entity Type	Non-profit
Entity 4	Entity Name	VU/A
	Role	Data processor
	Address	De Boelelaan 1105, 1081 HV Amsterdam, Nederland
	Contact(s)	Roderick van der Weerd: <a href="mailto:r.p.vander.weerd@vu.nl">r.p.vander.weerd@vu.nl</a>
	Entity Type	Non-profit
Structure of responsibility		For NEXT building (residential) and VIDEOLAB building (Commercial) VolkerWessels (via Hyrde) will be responsible for collecting data from persons, apartment and building level sensors and devices, via granted access from data owner. Anonymised data will be processed and forwarded to other involved pilot partners.
2.3 Rules and procedure		
Meetings		Regular pilot meetings, intercompany meetings/checks, and meetings organised in consortium (i.e., General assembly). In case of incidents specific meetings will be organized
Nomination		Agreement of data sharing among involved pilot partners
Publication of minutes		Presentations and defined tasks (via e-mail or in MS teams)
2.4 Continual improvement and periodic update		
Meetings		Regular pilot meetings, intercompany meetings/checks, and meetings organised in consortium (i.e., General assembly).
Evaluation procedure		During pilot meetings the evaluation is possible. And after the 3rd workshop evaluation will also be done.

3 DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.	
3.1	Pilot needs and resources for security and privacy data management
Ownership of data	Hyrde: for the Dutch pilot the application that is used to gather all event data is Ekco IoT platform.



PII Controller	<p>Hyrde: Ekco IoT platform purposes is to ingest event data related to energy and sensors from specific building, floor, home, room, or assets like PV panels and EV chargers. Gather insights from this data, and anonymize data for sharing as services to the InterConnect framework and Knowledge engine. Also end user preferences and feedback from the InterConnect App and iOffice app (part of Ekco App) is included and seen as event data.</p> <p>See Figure 31.</p> <p>The Ekco IoT platform consists of multiple sub-system(s) components - Ekco Builda, Ekco IoT, Ekco Control (BMS), Ekco Data lake, Ekco App, Ekco Hyrde gateway - making up the functional elements of the Ekco label, each hosted in the same secure cloud environment(s) as a Ekco IoT platform product.</p>	
PII Processors	<p>SmartThings cloud: process event data based from sensors for good functioning of the SmartThings app.</p> <p>TNO Reflex: process with their energy platform energy related to reduce energy consumption.</p> <p>Priva BMS; based on the Ekco control function the building management system is steered. this can include end user feedback about the climate.</p> <p>VU Amsterdam Forecaster: process event data to create AI models and forecasting predictions.</p>	
PII Principals	<p>Videolab; Facility Management, Building Owners, Community Manager</p> <p>Next; Residents/Consumers / Homeowners.</p>	
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		<p>Videolab; Facility Management, Building Owners, Community Manager</p> <p>Next; Residents/Consumers / Homeowners</p> <p>SmartThings -&gt; Ekco; we have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site (including data obtained in the context of InterConnect). Ekco receives from the SmartThings cloud event data that used for analysis and combinations of data in the pilot.</p> <p>The residents/building users that are the producers of data have all gave approval by approving the SmartThings agreement via the SmartThings app. By this they give consent to share their event data.</p> <p>Ekco -&gt; TNO reflex: a general data processing agreement is necessary between the Dutch Pilot partners and subcontractors.</p> <p>Ekco -&gt; VU Amsterdam: a general data processing agreement is necessary between the Dutch Pilot partners and subcontractors.</p> <p>IPR and confidentiality agreement</p> <p>Besides the 3 or 4 DPIAs (iCity, Hyrde, TNO, VUA) also a “agreement with a joint controller” is likely needed.</p>
Agreement 1	Organizations	Identification of the organizations concerned by the agreement.
	Agreement template	<p>Define the agreement template:</p> <ul style="list-style-type: none"> <li>Contract for collaboration with external companies.</li> <li>Pilot contract with residents/homeowners.</li> <li>Pilot contract with iOffice / Park Strijp Beheer.</li> <li>Data Processing Agreement.</li> <li>Consent form for residents/ homeowners/ end users.</li> </ul>
3.2.2	Data description	
Data 1	Dates for collection	To be specified.
	Identification of data	<ul style="list-style-type: none"> <li>Energy monitoring: <ul style="list-style-type: none"> <li>Khw per floor of the offices,</li> <li>Energy consumption smart meter,</li> <li>Energy consumption electricity,</li> <li>Khw solar panels,</li> <li>Khw charging lounge.</li> </ul> </li> <li>Building management: <ul style="list-style-type: none"> <li>Ventilation, heating, CO2, temperature, etc.</li> <li>Smart meter data</li> <li>Energy consumption</li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>○ Water consumption</li> <li>○ Light consumption</li> <li>• Homes and Apartments: <ul style="list-style-type: none"> <li>○ Motion,</li> <li>○ Water leak sensor,</li> <li>○ Wash machine,</li> <li>○ Door open/close,</li> <li>○ Temperature,</li> <li>○ Air quality</li> <li>○ Light</li> <li>○ Appliance's data</li> </ul> </li> <li>• Offices and workplace <ul style="list-style-type: none"> <li>○ Occupancy meeting rooms</li> <li>○ Counting people</li> <li>○ Occupancy</li> <li>○ Cleaning feedback</li> <li>○ Tickets</li> <li>○ Reservations</li> </ul> </li> </ul> <p>Service usage in energy services and smart home services. On a household and where applicable device/home appliance level. Type of services used, logged interactions with the technology.</p> <p>Consumer preferences regarding developed products and services: attitudes, perceived drivers and barriers, intention to buy.</p> <p>Usage data of smart devices (mainly household appliances like dish washer, washing machine and dryer). Switching on/off time. Programmed start time.</p> <p>Sensor data at home:</p> <ul style="list-style-type: none"> <li>• Smart meter data / energy use, per 15 minutes and real-time.</li> <li>• Motion: real time movement yes/no.</li> <li>• CO2 level, temperature, humidity, smoke detector, multiple times per hour.</li> </ul>
Type of data		<ul style="list-style-type: none"> <li>• PII (Personally Identifiable Information) Name, address, phone number, user id,</li> <li>• Business data; all event data, sensor data, system data, Ekco BMS data and end user feedback.</li> </ul>
Life Cycle		<ul style="list-style-type: none"> <li>• The data is captured through the Fiware reference architecture, by implementing the Orion context broker. Through our IoT agents the data is stored in EKCO core.</li> <li>• Data maintenance is performed by data models that are related to the Fiware architecture. These data models were decoded and values can use for different purposes.</li> <li>• Storage of data at a timeseries database makes it possible to do historical reporting in the future. Also monitoring if there is still data coming is part of this process.</li> <li>• Data Synthesis is done by the Ekco platform where multiple data streams are combined and used for performance of the building.</li> <li>• Data usage by the Ekco platform and mobile apps is done from event related data, also described as 'if this then that'. End users can directly act with this approach or automate their actions by implementing rules, scenes, and themes.</li> <li>• Data analytics - forecasting predictive models based on historical data is done with AI models. These models are later back implemented at the Ekco data usage level.</li> <li>• Data archiving - historical data is not used anymore but archived.</li> <li>• Deletion process - Data is deleted after a period of X months.</li> </ul>
Data description		 <p><b>FIGURE 32: DATA FLOW AND SPECIFICATION OF DUTCH PILOT</b></p>

3.2.3	Data exchange
Data flow	 <p><b>FIGURE 33: DATA FLOW DIAGRAM OF DUTCH PILOT</b></p>
Data access control chart	<p>The following roles have we defined with certain roles and permissions:</p> <ul style="list-style-type: none"> <li>• Users: create event data and share within the pilot.</li> <li>• Stakeholders: use the event data and analytics to perform services for end users.</li> <li>• Admin: store and processing data.</li> <li>• Operator: interpret the data for the pilot and add rules and logic to it - transform data into actions.</li> <li>• Analyst - subscribe to data for analytics and forecasting.</li> </ul>  <p><b>FIGURE 34: DATA ACCESS CONTROL CHART OF DUTCH PILOT</b></p>
3.2.4	Data access monitoring
Data access verification procedure	<p><b>Azure environment</b></p> <p>For the Dutch pilot the Microsoft Azure Cloud services under the Hyrde subscription account - part of the Microsoft Azure VolkerWessels Tenant contract-for provisioning, hosting, and serving the application service(s) and data lake storage. As it is commonly stated, Azure subscribes to various security requirements and participates in regular audits and has been certified against several compliance standards.</p> <p>Hyrde makes use of multiple data storage and databases technologies as part of the Ekco Data lake, depending on fit for purpose data processing and transformation capabilities required, some of the technologies include Fiware context broker, mongodb, quantum leap, Postgres and Azure SQL Database and Azure SQL Managed Instance services as part of their data warehousing strategy.</p>

In addition to Hyrde's internal data security structures, Azure provides clients with the following strategy and measures to ensure data security and contingency:

Microsoft Azure SQL Database and SQL Managed Instance provide a relational database service for cloud and enterprise applications. To help protect customer data, firewalls prevent network access to the server until access is explicitly granted based on IP address or Azure Virtual network traffic origin.

#### IP firewall rules

- IP firewall rules grant access to databases based on the originating IP address of each request.

#### Virtual network firewall rules

- Virtual network rules enable Azure SQL Database to only accept communications that are sent from selected subnets inside a virtual network.
- Authentication is the process of proving the user is who they claim to be. Azure SQL Database and SQL Managed Instance support two types of authentication.

#### SQL authentication

SQL database authentication refers to the authentication of a user when connecting to Azure SQL Database or Azure SQL Managed Instance using username and password. A server admin login with a username and password must be specified when the server is being created. Using these credentials, a server admin can authenticate to any database on that server or instance as the database owner. After that, additional SQL logins and users can be created by the server admin, which enable users to connect using username and password.

#### Azure Active Directory authentication

Azure Active Directory authentication is a mechanism of connecting to Azure SQL Database, Azure SQL Managed Instance and Azure Synapse Analytics by using identities in Azure Active Directory (Azure AD). Azure AD authentication allows administrators to centrally manage the identities and permissions of database users along with other Azure services in one central location. This includes the minimization of password storage and enables centralized password rotation policies.

A server admin called the Active Directory administrator must be created to use Azure AD authentication with SQL Database. For more information, see [Connecting to SQL Database by Using Azure Active Directory Authentication](#). Azure AD authentication supports both managed and federated accounts. The federated accounts support Windows users and groups for a customer domain federated with Azure AD.

Additional Azure AD authentication options available are Active Directory Universal Authentication for SQL Server Management Studio connections including Multi-Factor Authentication and Conditional Access.

Hyrde subscribes to both SQL and Azure Active Directory authentication. SQL authentication is set up for applications to access the data in the virtual network domain, while database management/administration is governed by using Azure Active Directory authentication.

#### Authorization

Authorization refers to the permissions assigned to a user within a database in Azure SQL Database or Azure SQL Managed Instance and determines what the user is allowed to do. Permissions are controlled by adding user accounts to database roles and assigning database-level permissions to those roles or by granting the user certain object-level permissions.

In addition to database-level authorization, Hyrde makes use of application layer roles and permissions to allow application users access to data. This is also logged as part of the data audit trail.

#### Threat protection

SQL Database and SQL Managed Instance secure customer data by providing auditing and threat detection capabilities.

SQL auditing in Azure Monitor logs and Events.

SQL Database and SQL Managed Instance auditing tracks database activities and helps maintain compliance with security standards by recording database events to an audit log in a customer-owned Azure storage account. Auditing allows users to monitor ongoing database activities, as well as analyse and investigate historical activity to identify potential threats or suspected abuse and security violations.

#### Advanced Threat Protection

Advanced Threat Protection is analysing your logs to detect unusual behaviour and potentially harmful attempts to access or exploit databases. Alerts are created for suspicious

	<p>activities such as SQL injection, potential data infiltration, and brute force attacks or for anomalies in access patterns to catch privilege escalations and breached credentials use. Alerts are viewed from the Azure Security Center, where the details of the suspicious activities are provided and recommendations for further investigation given along with actions to mitigate the threat.</p> <p><b>Information protection and encryption</b></p> <p><u>Transport Layer Security (Encryption-in-transit)</u></p> <p>SQL Database and SQL Managed Instance secure customer data by encrypting data in motion with Transport Layer Security (TLS). SQL Database and SQL Managed Instance always enforce encryption (SSL/TLS) for all connections. This ensures all data is encrypted "in transit" between the client and server irrespective of the setting of Encrypt or TrustServerCertificate in the connection string.</p> <p>In addition to DB TLS, all Hyrde application services are accessed using sha 256 RSA SSL certificates ensuring encrypted client to server communication.</p> <p><u>Transparent Data Encryption (Encryption-at-rest)</u></p> <p>Transparent Data Encryption (TDE) for Azure SQL Database and SQL Managed Instance adds a layer of security to help protect data at rest from unauthorized or offline access to raw files or backups. TDE encrypts the entire database using an AES encryption algorithm on cloud storage.</p> <p><b>Database backup</b></p> <p>Built into the Azure SQL Managed Instance is continuous database recovery and restoration options. Hyrde subscribes to a 7-day retention policy which enables system administrators to restore to a specific point in time.</p> <p>In addition to the built-in platform database recovery options, Hyrde has an off-line backup process where a full backup of the databases is encrypted and stored using off-line storage.</p>
3.2.5	Data Registry
Registry of agreements	Stored in data storage of involved companies.
Registry of data sets	To be specified.
Registry of citizen consents	To be specified.

4	Risk Management Plan
4.1	Pilot needs and resources for security and privacy risk management
Context for privacy analysis	Identify if a privacy analysis is needed (DPIA Threshold...).
Context for security analysis	Identify if a security analysis is needed.
Context for the project	Indicate whether there are common innovation capabilities from the consortium that you are using. Generic security and privacy capabilities will be supplied by the Consortium.
4.2	Risk management process
4.2.1	Security
Methodology	<ul style="list-style-type: none"> <li>Business Impact Assessment, incl. classification of Confidentiality, integrity, and availability of VolkerWessels.</li> <li>ISO 27001 methodology.</li> </ul>
Schedule	Regular pilot meetings, intercompany meetings/checks and meetings organised in Consortium (i.e., General Assembly). And participation of meeting 3 security and privacy risk analysis.
Template	Business Impact Assessment from VolkerWessels to be compared/combined with NEXT building owners BIV matrix/process.
4.2.2	Privacy
Methodology	Identify the privacy risk analysis methodology used:



	Business Impact Assessment, incl. classification of Confidentiality, integrity, and availability. ISO 27001 methodology.
Schedule	Regular pilot meetings, intercompany meetings/checks and meetings organised in Consortium (i.e., General Assembly). And participation of meeting 3 security and privacy risk analysis.
Template	Business Impact Assessment from VolkerWessels to be compared/combined with NEXT building owners BIV matrix/process.

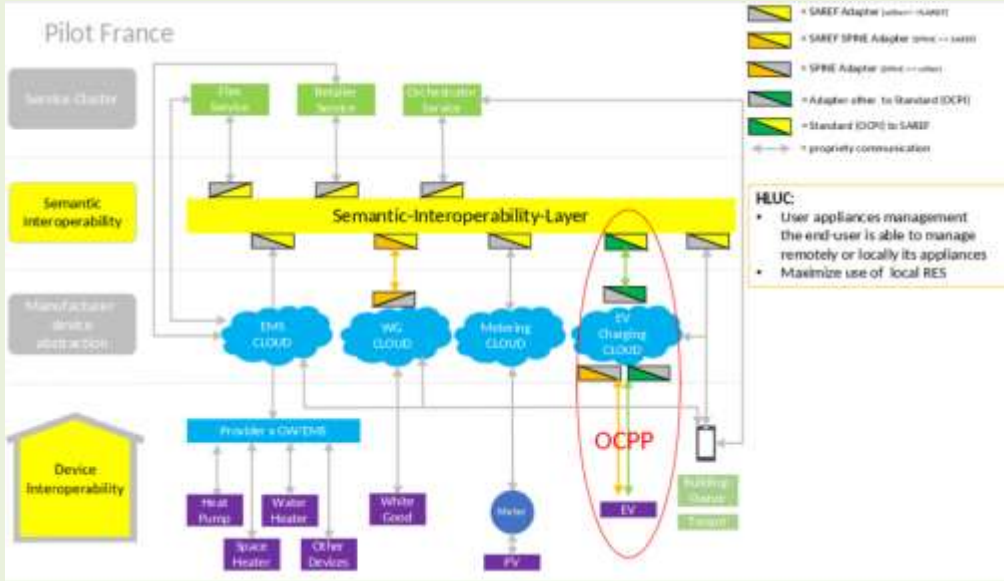
5 Engineering Management Plan	
Pilot needs and resources for security and privacy engineering	<p>Identify the current security and privacy capabilities, competences, persons to be allocated (security architecture, tools to help architects of developers to ensure security-by-design). Identify the common innovation capabilities that will be used (e.g., interoperability framework, access control, DLTs...).</p> <p>Check the need to use the INTERCONNECT unified access control capability.</p> <p>Ekco IoT platform and the multiple sub-system(s) components making up the functional elements of the Ekco label, each hosted in the same secure cloud environment(s) as the Ekco IoT platform product.</p> <p>Current security and privacy capabilities include:</p> <ul style="list-style-type: none"> <li>• Technical measures, encryption techniques and pseudonymisation techniques.</li> <li>• Re-use available results and methodology from InterConnect.</li> <li>• Data to be anonymized and the design of the pilot accordingly.</li> <li>• No security problems foreseen if services from the InterConnect framework are being used.</li> <li>• As mentioned, an incremental agreement for data sharing.</li> <li>• Risk analysis under Excel.</li> </ul>
Engineering process	Use Engineering process from the InterConnect project.
Schedule	<p>This can include WP5 proposal on common innovation capabilities to be used by the pilot.</p> <ul style="list-style-type: none"> <li>• Pilot feedback and agreement.</li> <li>• Consequently, risk analysis.</li> <li>• Implementation.</li> </ul> <p>From April 2021, the risk analysis will be started for the Pilot site 1 - Videolab and implementation of the 4 floors, then the system design task and finally the implementation, deployment and data collection starting, monitoring services.</p> <p>The risk analysis will be refined from Sprint 10 of the delivery and during rollout of the Pilot site 2 - NEXT apartment building and 150 apartments.</p>

6 Citizen Management Plan	
Pilot needs and resources for management	Before the pilot starts, the residents/building users that are the producers of data have all signed an informed consent form, confirming that their personal data can be used for research (not limited to InterConnect).
Management process	<p>iOffice stakeholders (Facility management, community managers, cleaning, etc.) Before the pilot starts all stakeholders related to using the iOffice solutions and collecting data, will sign an informed consent that they have access to event data and with that needs to be used confidential.</p> <p>Residents/ owners</p> <p>Before the pilot starts, the residents/building users that are the producers of data have all signed an informed consent form, confirming that their personal data can be used for research (not limited to InterConnect).</p> <p>SmartThings -&gt; Ekco; we have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site (including data obtained in the context of InterConnect). Ekco receives from the SmartThings cloud event data that used for analysis and combinations of data in the pilot.</p> <p>The residents/building users that are the producers of data have all gave approval by approving the SmartThings agreement via the SmartThings app. By this they give consent to share their event data.</p>



	<p>Ekco -&gt; TNO reflex: a general data processing agreement is necessary between the Dutch Pilot partners and subcontractors.</p> <p>Ekco -&gt; VU Amsterdam: a general data processing agreement is necessary between the Dutch Pilot partners and subcontractors.</p>
Schedule	<p>From April 2021, the risk analysis will be started for the Pilot site 1 - Videolab and implementation of the 4 floors, then the system design task and finally the implementation, deployment and data collection starting, monitoring services.</p> <p>The risk analysis will be refined from Sprint 10 of the delivery and during rollout of the Pilot site 2 - NEXT apartment building and 150 apartments.</p>

## ANNEX 2.4 FRENCH PILOT SPP

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	FRENCH PILOT
SUMMARY	<p><b><u>The objectives of the different high-level use case are:</u></b></p> <ul style="list-style-type: none"> <li>Maximize the self-consumption of locally produced renewable energy for individuals and/or community.</li> <li>Minimize the cost of consumption by using smart appliances to consume during the best periods of the dynamic tariff.</li> </ul> <p><b>NOTE:</b> For more detailed information about HLUC (High Level Use Cases), see D1.3.</p>
DESCRIPTION	 <p><b>FIGURE 35: OVERVIEW ARCHITECTURE OF FRENCH PILOT</b></p> <p>On the static architecture, there is a part that is deployed on premise and a part deployed in the clouds. On premise, it concerns home or municipality and includes a set of end points and local Energy Management Systems. End points can be appliances manufacturers, EV charging points, smart meter Linky, PV. All these end points will feed information back to the cloud, which will communicate data to the interoperability layer framework, and transfer this data to the smart orchestrator. The customer remains at all time the master of any service and can cancel/stop any order that he wishes with the help of the GUI. The advices from the smart orchestrator concerns the efficiency energy management. Then the EMS are responsible to automatically actuate the appliances according to the recommendation from the smart orchestrator and its authorization. Each EMS needs to send the actualized information to the smart orchestrator. The flexibility manager gets the data it needs to forecast the flexibility and needs real time update to adapt its forecast. The flexibility is activated in the pool by controlling the individual devices according to the requested flexibility from the energy market.</p> <p><b>Orchestrator</b></p> <ul style="list-style-type: none"> <li>To recommend new daily power load schedules,</li> </ul>

- To monitor local renewable energy production and recommend energy consuming equipment to consume in certain periods of time with the final target is to maximize local RES consumption;
- To control current home consumption load and avoid smart meter tripping by stopping load when necessary, according to user preferences.
- To manage the RES community: definition of the community, aggregation in real time of energy produced and energy consumed.

#### **White goods**

The Whirlpool washer energy flexibilities are:

- Power profile exposure of the scheduled washing programs of each smart device: the washer can expose by cloud API to Living or Energy Manager which washing sequences are scheduled: start time, end time, number of slots/phases, slot duration, slot Power consumption, etc.
- Load shifting command: possibility to reschedule from the Living Service Manager or Energy Manager API the washing program sequence set by the end-user, such as changing the start time (anticipate or delay).

*NOTE: It is not possible to issue a direct remote start or stop command, it is not possible changing the washing type of program / setpoint by cloud API such as ECO or RAPID option, this is prevented by design.*

#### **FLEX MANAGER (TV)**

- Leveraging data to forecast the thermal heating demands and available flexibility.
- Provide energy- and cost-efficient steering on appliances level, considering (time-varying) electricity prices, thermal losses, and household tariff incentives (e.g., self-consumption of local PV power). To this end, when multiple energy managers are active within a single household, a best-effort steering schedule is formulated by each energy manager. In case of day-ahead or intra-day forecasting errors, the orchestrator should overrule consumption state of the most appropriate appliance.
- Operate a Virtual Power Plant, providing value on the day-ahead, balancing, capacity and ancillary services market. To this end, an aggregate baseline and flexibility schedule for the entire pool of appliances is identified and updated in real-time.

#### **FLEX MANAGER (ENGIE)**

The flexibility manager:

- gets the data it needs to forecast the flexibility
- needs real time update to adapt its forecast
- activates flexibility in the pool according to the requested flexibility
- gets real time feedback from portfolio to adapt the flexibility dispatch
- The customer can disable the flexibility if required.

#### **eV CHARGING PLATFORM**

- Allow the user to configure the EV platform.
- Offer the possibility to get information about current events occurring through the EV platform.
- Provide the planned charging schedules for the connected EVs as well as the schedule of the global system.
- Allows a flexibility to manage to receive flexibility offers and demand schedule adaptations.
- Offer functionalities that can only be used for a user with special rights.

#### **METERING DATA PLATFORM Main features**

- receive incoming data from the smart meter in real time (tariff index, subscribed power and instantaneous power, virtual contact) via a radio transmitter (ERL) device (over Wi-Fi)
- dispatch the information coming from the smart meter to the smart orchestrator platform (over IP), EV charging platform (over IP)

*The provision of data in real time cannot be achieved without the consumer consent.*

#### **SGE ENEDIS**

SGE\* ("Système de Gestion des Échanges") is a web platform for data exchange between Enedis and market players. Since 2004, it has been the tool that enables suppliers to request and track services ordered from Enedis (commissioning, power changes, etc.). It is also open to third-party companies to enable them to access individual data independently.

\*TIC = "Télé Information clients" = Remote information to the customer

'SGE' = 'Système de Gestion des Échanges' = Exchange Management System

#### **EMS - Features**

- Collect user preferences relative to his comfort. The EMS proposes general terms and ad-hoc rules, such as temperature into a room, temperature planning, etc. to enable the user to express his preferences.

	<ul style="list-style-type: none"> <li>Collect data measuring the context in which the house's devices are set by the end-user: energy consumption, target temperature into the house, instantaneous power, etc.</li> <li>Send ad-hoc rules and collected data to the Smart Orchestrator, which guarantees the consistency of the whole system and sends back optimized consumption schedule recommendation to the EMS, considering dynamic tariff incentives and maximum power.</li> <li>Actuate the devices that it manages (starting or stopping them by following device features), in consideration of the consumption schedule recommendation sent by the EMS. To start a device, the EMS must request authorization from the smart orchestrator.</li> <li>Provide flexibility to the grid: <ul style="list-style-type: none"> <li>Calculate the planned consumption of all the devices that it manages.</li> <li>Send this planned consumption to the Flex Manager/smart orchestrator.</li> <li>Receive the flexibility request from the Flex Manager and applies it to the house's devices.</li> <li>Report to the Flex Manager the application of the flexibility.</li> </ul> </li> </ul> <p>PUC (Pilot Use Case) 1</p> <p>The photovoltaic solar panels produce energy. The production information is transmitted to the system by the metering system.</p> <p>PUC2</p> <p>The objective is to consider the needs of the user to identify the best time to activate the end users.</p> <p>PUC3</p> <p>Provide contracts to consumers. Associating consumers and producers around a local production project or for dynamic tariff use.</p> <p>PUC 4</p> <p>Activate EV and appliances in consideration of the Smart Orchestrator recommendations. This PUC aims to operate the appliances, the white goods and EV charging optimally.</p> <p>PUC 5</p> <p>This use case involves an IT component that produces home level recommendations related to consumption scheduling and power limitation.</p> <p>PUC6</p> <p>Piloting modules will modify the consumption of different devices (like water heaters, space heaters, heat pumps, etc.) according to 1) comfort, 2) energy efficiency, 3) dynamic tariff or MAX RES 4) flexibility. The end user needs to be able to interrupt the piloting to take back over the hand on the control.</p> <p>PUC7</p> <p>The retailer calculates and provides a dynamic tariff to customer or smart orchestrator.</p> <p>PUC 8</p> <p>A Flexibility Service Provider (FSP) evaluates the flexibility capacities and provide flexibility to the TSO in the framework.</p>
--	--

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation	GDPR <a href="#">CEER document for dynamic tariff specification</a> CNIL n ° 2012-404 of November 15th, and decree n ° 2019-536 of May 29, 2019 The Linky system respect ANSSI recommendations CNIL compliance pack for smart meters <a href="https://www.cnil.fr/sites/default/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf">https://www.cnil.fr/sites/default/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf</a>	
International Standards	W3C IC 62056.3.1 (communication protocol; downstream smart meter communication, when connected to an EMS with cable, the data format of the smart meter information is described in this format) Take into consideration with the ISO and make some recommendation to the EC: ISO 27xxx family of standards that we can investigate.	
2.1 GOVERNANCE BODY		
Information Manager	Security	To be specified.

Data Protection Officer		To be specified.
Other roles		To be specified.
Ecosystem consideration		To be specified.
2.2 ORGANISATION RESPONSIBILITY		
Entity 1	Entity Name	Yncrea
	Role	French pilot leader
	Address	Maison des technologies, Place Georges Pompidou, 83000 Toulon
	Contact(s)	Stéphane Vera : ( <a href="mailto:stephane.vera@yncrea.fr">stephane.vera@yncrea.fr</a> ); Anais Galligani : ( <a href="mailto:anais.galligani@yncrea.fr">anais.galligani@yncrea.fr</a> )
	Entity Type	Research Institute
Entity 2	Entity Name	ENGIE
	Role	Provide dynamic tariff & flexibility
	Address	1 PLACE SAMUEL DE CHAMPLAIN, COURBEVOIE 92400, France
	Contact(s)	Marc Lelandois : ( <a href="mailto:marc.lelandois@external.engie.com">marc.lelandois@external.engie.com</a> ); Martin Manon : ( <a href="mailto:manon.martin@engie.com">manon.martin@engie.com</a> )
	Entity Type	Energy Retailer
Entity 3	Entity Name	Trialog
	Role	Provide T-EMS to manage EV charging
	Address	25 Rue du Général Foy 75008 PARIS (France)
	Contact(s)	Frédéric Mesureur : ( <a href="mailto:Frederic.mesureur@trialog.com">Frederic.mesureur@trialog.com</a> ); Dune Sebillieu : ( <a href="mailto:dune.sebillieu@trialog.com">dune.sebillieu@trialog.com</a> )
	Entity Type	SME
Entity 4	Entity Name	GFI World/Inetum
	Role	Develop the smart Orchestrator
	Address	A VAUCAMPSLAAN 42, HUIZINGEN 1654, Belgium
	Contact(s)	Sylvain Rival : ( <a href="mailto:sylvain.rival@gfi.world">sylvain.rival@gfi.world</a> ) María Pérez : ( <a href="mailto:maria.perez@gfi.world">maria.perez@gfi.world</a> )
	Entity Type	Consultancy
Entity 5	Entity Name	Thermovault
	Role	Provide ancillary flex to RTE (French TSO) + install smart devices to monitor thermal devices
	Address	HOEFSTADSTRAAT 86, GENK 3600, Belgium
	Contact(s)	Sandro Iacovella : ( <a href="mailto:sandro.iacovella@thermovault.com">sandro.iacovella@thermovault.com</a> ); Marc Shicks : ( <a href="mailto:marc.schicks@thermovault.com">marc.schicks@thermovault.com</a> )
	Entity Type	SME
Entity 6	Entity Name	Enedis
	Role	Will develop the smart metering platform
	Address	34 PLACE DES COROLLES TOUR ERDF, PARIS LA, DEFENSE CEDEX 92079
	Contact(s)	Romain Bonnin : ( <a href="mailto:romain-externe.bonnin@enedis.fr">romain-externe.bonnin@enedis.fr</a> ) Matthieu Rubion : ( <a href="mailto:matthieu.rubion@enedis.fr">matthieu.rubion@enedis.fr</a> )
	Entity Type	French DSO
Structure of responsibility		To be specified.

2.3	Rules and procedure	
Meetings	Weekly each Monday: 2 to 4 pm CET.	
Nomination	To be specified.	
Publication of minutes	To be specified.	
2.4	Continual improvement and periodic update	
Meetings	To be specified.	
Evaluation procedure	To be specified.	

In this section, the data management plan has been specified partner by partner involved in the collection and treatment of data. Then, the project presents four tables, one per partner involved, highlighted the name in white colour.

<b>3 DATA MANAGEMENT PLAN ENEDIS</b>		
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	Smart meter data: In the French law, "ownership of data" title is not recognized. The customer/ client is the meter data holder.	
PII Controller	Real time smart meter data: The controller is the third party who signs a contract, provides a service, and exploits the data of the customer/ client.	
PII Processors	Engie/Trialog for dynamic tariff (HLUC2) Thermovault /Inetum / Trialog / Yncrea for Max RES (HLUC 1)	
PII Principals	The client is the meter data principals.	
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach	Smart meter data: Article R.111-27 of the Energy Code specifies that the DSO can transmit data to a third party as soon as it has received consent from the customer.	
Agreement 1	Organizations	Smart meter data: the service provider who exploits the meter data in real time is responsible for data management.
	Agreement template	Any third-party actor transmits a client's consent to the DSO may collect data from the meter data platform. The client's consent must be specified in the contract signed between the service provider and the client.
3.2.2	Data description	
Data	Dates for collection	Smart meter data: the platform continuously collects meter data from ICT. And the client consent authorizes the service provider to collect the data from the DSO platform for a limited period (one year).
	Identification of data	Real time smart meter data: customer's data is identified from the client smart meter (PDL identification: unique smart meter identification code).
	Type of data	Real time smart meter data is PII and Business data.
	Life Cycle	Smart meter data in real time: The data is not stored in the platform, it is a continuous flow. The flow sent to the interoperability layer is anonymized.

	Data description	<p><b>Smart meter data (TIC):</b></p> <ul style="list-style-type: none"> <li>• Client contract information</li> <li>• PDL (identification code).</li> <li>• Power subscribed.</li> <li>• Type of contract (off-peak hours, etc.).</li> <li>• Supplier management usage signals (virtual contacts).</li> </ul> <p><b>Customer consumption data:</b></p> <ul style="list-style-type: none"> <li>• Instantaneous kW power drawn.</li> <li>• The maximum power reached during the day.</li> </ul> <p><b>Customer production data:</b></p> <ul style="list-style-type: none"> <li>• The instantaneous power kW produced by the installation.</li> <li>• The maximum power reached during the day.</li> <li>• PDL: unique identifier code of the subscription of the home; for energy provider + Enedis</li> </ul>
3.2.3	Data exchange	
Data flow	Real-time data from the smart meter is retrieved and transmitted to the platform via a simple modem connected to the meter's ICT. The third-party actor connects to the anonymized meter data platform to collect and use the data.	
Data access control chart	To be specified.	
3.2.4	Data access monitoring	
Data access verification procedure	Smart meter data: Real-time meter data can be retrieved from the meter data platform by third party actors when it provides to the DSO the proof of customer consent and the customer's PDL number (identification code).	
3.2.5	Data Registry	
Registry of agreements	Smart meter data: The meter data platform transmits the anonymized data to third parties but does not store meter data.	
Registry of data sets	<p>The data below are not stored.</p> <p>They are anonymised by using cryptographic mechanism on PDL.</p> <ul style="list-style-type: none"> <li>• Client contract information <ul style="list-style-type: none"> <li>○ PDL (identification code)</li> <li>○ Power subscribed.</li> <li>○ Type of contract (off-peak hours, etc.)</li> <li>○ Supplier management usage signals (virtual contacts)</li> </ul> </li> <li>• Customer consumption data: <ul style="list-style-type: none"> <li>○ Instantaneous kW power drawn.</li> <li>○ The maximum power reached during the day.</li> </ul> </li> <li>• Customer production data: <ul style="list-style-type: none"> <li>○ The instantaneous power kW produced by the installation.</li> <li>○ The maximum power reached during the day.</li> </ul> </li> </ul>	
Registry of citizen consents	Smart meter data: The customer's consent must be stated in the service provider's contract and stored in the service provider's database.	

3	DATA MANAGEMENT PLAN ENGIE	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	The customer owns the data	
PII Controller	ENGIE	
PII Processors	Subcontractors: Trialog, Tiko, Inetum	
PII Principals	Identification of the PII Principals in the application context. Residents and building users.	



3.2		Data Management Process
3.2.1		Agreements
Agreement approach		Smart meter data: Article R.111-27 of the Energy Code specifies that the DSO can transmit data to a third party as soon as it has received consent from the customer. Agreement between the PII processors and ENGIE.
Agreement 1	Organizations	<ul style="list-style-type: none"> <li>Data sharing agreement between ENGIE and Trialog for flexibility offers and summary of energy really consumed.</li> <li>Data sharing agreement between ENGIE and Inetum for dynamic tariff.</li> </ul>
	Agreement template	To be defined based on H2020 grant agreement.
3.2.2		Data description
PII	Dates for collection	Date when collection starts and ends: Q4-2021 to Q4 2023.
	Identification of data	<ul style="list-style-type: none"> <li>Customer identity (name, address, phone numbers, mail address).</li> <li>PoD (Point of Delivery= PDL (Point De Livraison).</li> <li>Customer settings: temperature, preferences on comfort, savings, environmental concerns, usage timetable.</li> <li>Instantaneous power: real-time power consumed into the house.</li> <li>Home load curves: 48 values of average power (2 per/hour).</li> <li>Energy contract: Contract describing Energy services.</li> <li>InterConnect contract: Contract describing appliances steering according to dynamic tariff optimization and grid flexibility.</li> <li>Appliances load curves (load curves of heaters and boiler).</li> <li>Internal temperature time series.</li> <li>Flexibility refusals.</li> </ul>
	Type of data	The data is: <ul style="list-style-type: none"> <li>PII (Personally Identifiable Information)</li> <li>It also concerns Business data and service data.</li> </ul>
	Life Cycle	The life cycle of the data will be detailed by the Privacy by Design to be defined next month by ENGIE. The storage time: depends on the type of data: between one year and the duration of the contract. There is a deletion process depending on the applications.
	Data description	PDL: unique identifier code of the subscription of the home; for energy provider and Enedis.
Business Data	Dates for collection	Date when collection starts and ends: Q4-2021 to Q4-2023
	Identification of data	Dynamic tariff: tariff provided by ENGIE from 24-hour Spot prices and ENGIE commercial policy.
	Type of data	The data is: <ul style="list-style-type: none"> <li>Business data</li> <li>Critical to service data</li> </ul>
	Life Cycle	The life cycle will be detailed by the Privacy by Design to be defined next month by ENGIE. The storage time: depends on the type of data: between one year and the duration of the contract. There is a deletion process depending on the applications.
	Data description	Price by hour (Euros/kWh).
Data critical to service	Dates for collection	Date when collection starts and ends: Q4-2021 to Q4-2023
	Identification of data	<ul style="list-style-type: none"> <li>Appliance's flexibility</li> <li>EV flexibility</li> </ul>
	Type of data	The data is Critical to service data.

	Life Cycle	<p>The data life cycle will be detailed by the Privacy by Design to be defined next month by ENGIE.</p> <p>The storage time depends on the type of data, between one year and the duration of the contract.</p> <p>There is a deletion process depending on the applications.</p>
	Data description	Appliance's flexibility and EV flexibility are energy consumption planned in the house and on the EV (kWh by hour). The format must be defined.
3.2.3	Data exchange	
Data flow	<p><b>FIGURE 36: DATA FLOW DIAGRAM OF ENGIE DATA</b></p>	
Data access control chart	Dynamic tariff, home load curves and appliances load curves are only shared with the smart Orchestrator.	
3.2.4	Data access monitoring	
Data access verification procedure	The ENGIE security policy is applied.	
3.2.5	Data Registry	
Registry of agreements	Agreements are stored safely by ENGIE into its Cloud.	
Registry of data sets	Data sets are stored safely by ENGIE into its Cloud.	
Registry of citizen consents	Consents are stored safely by ENGIE into its Cloud.	

3	DATA MANAGEMENT PLAN INETUM/YNCREA	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	<p>Numerous data should be provided to the smart Orchestrator (SO). Following table indicate which entity is the owner of the data (refer to each partner section to retrieve data source and management). The SO provides data that are the results of calculation based on partner's data. Such data is attached to the Home ID which do not handle any privacy information.</p> <p><b><u>Engie/ThermoVault:</u></b></p> <ul style="list-style-type: none"><li>• Home configuration.</li><li>• Zip code.</li><li>• Energy performance class.</li><li>• User preferences (also Trialog).</li><li>• Comfort thresholds (also Trialog).</li><li>• Appliances ID.</li><li>• Tariff dynamic.</li><li>• House load curves.</li><li>• Aggregated load curve of heaters.</li><li>• Load curve of boilers.</li><li>• Stop period.</li></ul>	

		<p><b><u>Inetum:</u></b></p> <ul style="list-style-type: none"> <li>Power limitation threshold.</li> <li>Total potential savings for a day in € and in CO2 emissions.</li> <li>Order type.</li> <li>Consume RES.</li> <li>Recommended load curve.</li> </ul> <p><b><u>Enedis:</u></b></p> <ul style="list-style-type: none"> <li>Instantaneous power consumed.</li> <li>Instantaneous power produced.</li> <li>PV production signal.</li> </ul> <p><b><u>Yncrea:</u></b></p> <ul style="list-style-type: none"> <li>Community ID.</li> <li>Community description.</li> <li>Consume RES.</li> </ul> <p><b><u>Trialog:</u></b></p> <ul style="list-style-type: none"> <li>FlexOffer.</li> <li>Load curve of EV charging wall boxes.</li> <li>User preferences.</li> <li>Comfort thresholds.</li> </ul> <p><b><u>InterConnect:</u></b></p> <ul style="list-style-type: none"> <li>Home ID.</li> <li>Traffic light.</li> </ul>
PII Controller		Each partner controls its own data (Refer to each partner section to retrieve data source and management).
PII Processors		Inetum, Yncréa, Engie, Trialog, ThermoVault, manufacturer backends.
PII Principals		Refer to each partner section to retrieve data source and management.
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach		<p>Refer to each partner section to retrieve data source and management.</p> <p>Smart meter data: Article R.111-27 of the Energy Code specifies that the DSO can transmit data to a third party as soon as it has received consent from the customer.</p> <p>Contract signed by customer containing the data management process.</p>
Agreement 1	Organizations	Engie, Enedis, Trialog, ThermoVault
	Agreement template	To Be Done: based on existing customer contract.
<b>3.2.2 Data description</b>		
Data	Dates collection for	<p>Data underneath are created one time when a home is instantiated:</p> <ul style="list-style-type: none"> <li>Home ID (anonymized in the data source).</li> <li>Home configuration.</li> <li>Zip code.</li> <li>Energy performance class.</li> <li>Appliances ID.</li> </ul> <p>Data underneath are created one time when a community is instantiated:</p> <ul style="list-style-type: none"> <li>Community_ID.</li> <li>Community_Description.</li> </ul> <p>All other data are collected or provided daily from the beginning of the project or real time values upon requests.</p>
	Identification of data	Data are identified by the Home ID and Community ID. The Home ID and Community ID do not carry out any privacy information and does not allow to identify the user.
	Type of data	<ul style="list-style-type: none"> <li>Business data.</li> </ul>

		<ul style="list-style-type: none"> <li>Critical to service data.</li> </ul>
	Life Cycle	Storage time - see table. Deletion process - scheduled DB process.
	Data description	See document 62559_PUC5_Smart Orchestrator processing & operations related to the French pilot.
3.2.3	Data exchange	
Data flow	See sequence diagram included in document 62559_PUC5_Smart Orchestrator processing & operations related to the French pilot.	
Data access control chart	There is no access to any data directly by persons. The data are exchanged by using the interoperability layer.	
3.2.4	Data access monitoring	
Data access verification procedure	Since the data are exchanged throughout the interoperability layer the access is managed by interoperability layer and the associated registering process. Data integrity is guarantee by design.	
3.2.5	Data Registry	
Registry of agreements	The SO does not interact with user. Refer to each partner section to retrieve data source and management.	
Registry of data sets	Refer to life cycle section.	
Registry of citizen consents	The SO does not interact with user. Refer to each partner section to retrieve data source and management.	

3	DATA MANAGEMENT PLAN THERMOVAULT		
InterConnect data management plan is the first input.			
3.1	Pilot needs and resources for security and privacy data management		
Ownership of data		ThermoVault owns data produced by thermal appliances.	
PII Controller		ThermoVault is the PII controller of the thermal appliances data.	
PII Processors		Inetum, Trialog, Yncréa	
PII Principals		Residents and building users.	
3.2	Data Management Process		
3.2.1	Agreements		
Agreement approach		ThermoVault and the tenants have a mutual agreement, fixed in a contract, regarding the controlling and processing of personal data on the pilot site. The residents/building users that are the producers of data have all signed an informed consent form, which needs to be extended specifically to the InterConnect project. In addition, a data processing agreement with the White-good, and EMS providers will need to be made in the informed consent form.	
Agreement 1	Organizations	ThermoVault and the end user	
	Agreement template	A template contract between the parties ThermoVault and the end users.	
3.2.2	Data description		
Data	Dates collection for	Expected Q4 2021 start of data collection and sharing until the end of the project.	
	Identification of data	<ul style="list-style-type: none"><li>Electricity demand per site.</li><li>Boiler and space heaters electricity demand.</li><li>Room and water vessel temperature measurements.</li></ul>	

	Type of data	All data is PII and Critical to service data.
	Life Cycle	Data will be stored from Q4 - 2021 until the end of the project. Then it will be deleted.
	Data description	PDL: unique identifier code of the subscription of the home (anonymized); for energy provider + Enedis.
3.2.3	Data exchange	
Data flow	Thermal loads data previously described (Sec. 4.2.2) is not shared and ThermoVault produces a three-level signal to indicate the current available flexibility.	
Data access control chart	Thermal loads status data is shared in the interoperability layer and published frequently. Only the smart orchestrator can access to this data.	
3.2.4	Data access monitoring	
Data access verification procedure	The Smart orchestrator can access to the flexible asset status data through the interoperability layer and its security mechanisms.	
3.2.5	Data Registry	
Registry of agreements	Agreements are stored safely by ThermoVault.	
Registry of data sets	The list is stored safely by ThermoVault.	
Registry of citizen consents	Consents are stored safely by ThermoVault.	

3	DATA MANAGEMENT PLAN TRIALOG	
InterConnect data management plan is the first input		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	<ul style="list-style-type: none"><li>• EV owner acting as a flexibility provider (EV residential usages, EV city hall usages)</li><li>• EV user (for EV city hall usages only).</li><li>• Smart meter contract owner (customer).</li><li>• Flexibility service provider acting as Flexibility Manager/Retailer for dynamic tariffs (Engie).</li></ul>	
PII Controller	<ul style="list-style-type: none"><li>• Engie, sharing dynamic tariffs.</li><li>• ThermoVault for Max RES use case.</li></ul>	
PII Processors	<ul style="list-style-type: none"><li>• Yncrea academy acting as data collector and processor with the Smart Orchestrator.</li><li>• Inetum company acting as data collector and processor with the Smart Orchestrator.</li><li>• Engie company acting as flexibility manager, data collector and processor.</li><li>• Thermovault company acting as flexibility manager, data collector and processor.</li><li>• Trialog company acting as data collector and processor of PII from EV owner, EV user, Smart meter, dynamic tariffs.</li></ul>	
PII Principals	<p><b>EV owner</b></p> <p>This is the owner of the EV that consents to provide energy flexibility according to its EV personal and daily usages.</p> <p>This owner may has subscribed a specific tariff contract with its energy manager.</p> <p><b>EV user</b></p> <p>This is an EV user. The EV belongs to the city hall and is used in a professional setting providing flexibility.</p> <p><b>Smart meter contract owner</b></p> <p>This is the smart meter contract owner that consent to provide</p> <ul style="list-style-type: none"><li>• its maximum energy available in building.</li><li>• its energy instantaneous consumption.</li><li>• its energy production.</li></ul> <p><b>Energy contract owner</b></p>	

		<p>This is the energy contract owner that consent to provide tariff information granted from the Energy manager he has contractual agreements with.</p> <p><i>NB: Dynamic tariffs provided by the energy manager are not considered as PII since they are not personal (discussion in April between Trialog/ENGIE ).</i></p>
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		Agreement between data processors and data controllers.
Agreement 1	Organizations	<ul style="list-style-type: none"> <li>Data sharing agreement between Enedis and Trialog (PII Processor) for sharing TIC information.</li> <li>Data sharing agreement between the Charge points owner - Vinci Citeos and Trialog (PII Processor) for EV usages and EV charges.</li> <li>Data sharing agreement between Trialog and Engie (PII Processor) for flexibility offers and summary of energy really consumed -&gt; to be confirmed in April 2021.</li> <li>Data sharing agreement between Trialog and Inetum (PII Processor) for flexibility offers and summary of energy really consumed -&gt; to be confirmed following PUC5 alinement's (10/02/2021).</li> <li>Data sharing agreement between Inetum and Trialog (PII Processor) for classified index sharing as smart orchestrator.</li> </ul>
	Agreement template	Use template provided by the data controllers.
3.2.2	Data description	
Metering Data	Dates for collection	Every 1 second (minimum)
	Identification of data	<p>TIC Information</p> <ul style="list-style-type: none"> <li>Max power available (from contract).</li> <li>Instantaneous consumed power.</li> <li>Production (To be discussed in April 2021).</li> </ul>
	Type of data	<ul style="list-style-type: none"> <li>PII, since it provides user/owner consumption habits.</li> <li>Business data, for Enedis.</li> <li>Critical for service data, in a way it is an important piece of information for the TEMS service processing. It is not mandatory.</li> </ul>
	Life Cycle	<ul style="list-style-type: none"> <li>Storage time.</li> <li>Deletion process.</li> <li>Used for TEMS real time processing.</li> <li>Storage for TEMS data/user learning for a long period of time (~1 year).</li> </ul>
	Data description	PDL: unique identifier code of the subscription of the home; for energy provider + Enedis Information is extracted from the smart meter TIC by the Enedis metering service and exposed on the interoperability layer as a service.
Tariff Information	Dates for collection	Every 24 hours.
	Identification of data	<p>Tariff indexes per hour with their associated priority, from the most expensive (low priority) to the cheapest (high priority).</p> <p>Up to 8 hours before the actual time.</p>
	Type of data	<p>PII, since it provides owner electrical contract details.</p> <p>Business data, for ENGIE.</p> <p>Not critical to service data: it provides additional information for T-EMS service so it can be more accurate.</p>
	Life Cycle	<p>Data processed at every update and stored in between.</p> <p>Storage for TEMS data/user learning for a long period of time (~1 year). It requires an agreement with the data providers.</p>
	Data description	HomeID: unique identifier code for the subscription of the home; for energy provider + Enedis.



		These data are provided by the smart orchestrator through the interoperability layer.
Flexibility Offers	Dates for collection	For an outside system, the offers processing is event driven (timing, situation updates).
	Identification of data	To be specified.
	Type of data	<ul style="list-style-type: none"> <li>• PII, since it provides owner/user electrical consumption forecast.</li> <li>• Not business data (the monetization has been cancelled).</li> <li>• Not critical to service data: T-EMS can be used without the flexibility module, but it can be critical to outside services.</li> </ul>
	Life Cycle	The offers are stored for as long as they are valid.
	Data description	HomeID: unique identifier code for the subscription of the home; for energy provider + Enedis. See the flexibility protocol document (coming next).
Adaptation Demands	Dates for collection	Demands are event driven (timing, situation updates)
	Identification of data	Adaptation demands: <ul style="list-style-type: none"> <li>• based offers.</li> <li>• energy schedule for the system.</li> </ul>
	Type of data	<ul style="list-style-type: none"> <li>• PII, since it provides owner/user electrical consumption forecast.</li> <li>• Business data, for ENGIE.</li> <li>• Not critical to service data: T-EMS can be used without the flexibility module, but it can be critical to outside services.</li> </ul>
	Life Cycle	Stored until as long as they are valid (time, parameters)
	Data description	HomeID (anonymized): unique identifier code for the subscription of the home; for energy provider + Enedis. See the flexibility protocol document (coming next)
Data exchange with charge points	Dates for collection	Direct communication, response/request type.
	Identification of data	Data received from charge points: <ul style="list-style-type: none"> <li>• meter values (energy, power).</li> <li>• connection/disconnection.</li> <li>• end/beginning of session.</li> <li>• user id (token).</li> </ul> Data sent to charge points: <ul style="list-style-type: none"> <li>• energy/power schedules.</li> <li>• charge authorization.</li> </ul>
	Type of data	<ul style="list-style-type: none"> <li>• PII, since it provides owner/user id (token).</li> <li>• Business data, for us.</li> <li>• Critical to service data: mandatory for T-EMS operation.</li> </ul>
	Life Cycle	The current behaviour of T-EMS is to save all relevant information (session dates, power, etc.) from chargers in an internal database.
	Data description	HomeID (anonymized): unique identifier code for the subscription of the home; for energy provider + Enedis. See OCPP and EEBUS specifications.
Flexibility availability status	Dates for collection	For an outside system, the offers processing is event driven (timing, situation updates).
	Identification of data	T-EMS flexibility availability status (UNAVAILABLE, STANDBY, BEFORE_ADAPTATION, IN_ADAPTATION).
	Type of data	<ul style="list-style-type: none"> <li>• No PII.</li> <li>• No business data.</li> <li>• Not critical to service data: T-EMS can be used without the flexibility module, but it can be critical to outside services.</li> </ul>

	Life Cycle	The status represents the current availability state of the system. A new state overrides the old one.
	Data description	HomeID (anonymized): unique identifier code for the subscription of the home; for energy provider + Enedis. See the flexibility protocol document (coming next).
GUI Information	Dates for collection	(To Be Done) Direct communication, request/response system.
	Identification of data	Information retrieved from the user interface: <ul style="list-style-type: none"> <li>T-EMS configuration.</li> <li>User power configuration (min/max, time priorities).</li> </ul> Information sent to the user interface: <ul style="list-style-type: none"> <li>Power forecast.</li> <li>Monitoring service (power/energy, connected EVs, information relative to EVs).</li> </ul>
	Type of data	PII, since it provides owner/user power consumption forecast/monitoring, EV availability. Business data, for us. Not critical to service data: T-EMS can be used without the user interface. It is however an important source of additional information.
	Life Cycle	TEMS configuration is stored for all the duration of the system service, as well as the user preferences. The data sent to the user are managed by the user.
	Data description	HomeID (anonymized): unique identifier code for the subscription of the home; for energy provider + Enedis.
<b>3.2.3 Data exchange</b>		
Data flow		Check French pilot's PUC4 for a detailed sequence diagram.
Data access control chart		To be specified. (Data access through the interoperability layer with the exposed services. Does that require data access control managed by who? The smart orchestrator? Default InterConnect services? Could guaranty data access restriction such as room temperature of ThermoVault and dynamic tariffs of Engie? Why not! -> Should be mandatory for the French pilot. Agreement with the marketplace?) =>all these questions need to be answered in the m3 meeting.
<b>3.2.4 Data access monitoring</b>		
Data access verification procedure		This monitoring could be managed/provided by the Smart Orchestrator or could be part of elemental pack of services provided by InterConnect? To be decided -> Should be mandatory for the French pilot.
<b>3.2.5 Data Registry</b>		
Registry of agreements		On Trialog secure internal servers.
Registry of data sets		On Trialog secure internal servers.
Registry of citizen consents		On Trialog secure internal servers.

<b>4</b>	<b>Risk Management Plan</b>	
<b>4.1</b>	<b>Pilot needs and resources for security and privacy risk management</b>	
Context for privacy analysis		Yes, it is needed.
Context for security analysis		Yes, because of our use case (deployed in the customer household, buildings), we don't want the data to be modified, nor hacked. The system must be operational and secure.
Context for the project		The French pilot take advantage of InterConnect interoperability framework.
<b>4.2</b>	<b>Risk management process</b>	

4.2.1	Security
Methodology	We follow recommendations of D2.1
Schedule	<p>May 2021: start of the DPIA 1</p> <p>September 2021: security and privacy risk analysis meeting</p> <p>30th of September 2021: delivery of the DPIA</p> <p>1st October 2021 to 1st of November 2021 =&gt; setup demonstration V1</p> <p>From 3<sup>rd</sup> November 2021 to 15th April 2022: demo V1</p> <p>November 2021: start of the DPIA 2 if required</p> <p>1st April 2022: delivery of the DPIA 2</p> <p>from 18th April 2022 to 18th May 2022: setup demo v2</p> <p>From 19th May 2022 to 30th Sept 2022: demo V2</p> <p>1st May 2022: start of the DPIA 3 if required</p> <p>From 3<sup>rd</sup> Oct 2022 to 2nd of November 2022: setup demo V3</p> <p>2nd November 2022: delivery of the DPIA 3</p> <p>From 3<sup>rd</sup> of November 2022 to August 2023: demo V3</p>
Template	InterConnect template based on CNIL.
4.2.2	Privacy
Methodology	The French pilot follows the methodology described in D2.1.
Schedule	<p>May 2021: start of the DPIA 1</p> <p>September 2021: security and privacy risk analysis meeting</p> <p>30th of September 2021: delivery of the DPIA</p> <p>1st October 2021 to 1st of November 2021 =&gt; setup demonstration V1</p> <p>From 3<sup>rd</sup> November 2021 to 15th April 2022: demo V1</p> <p>November 2021: start of the DPIA 2 if required</p> <p>1st April 2022: delivery of the DPIA 2</p> <p>from 18th April 2022 to 18th May 2022: setup demo v2</p> <p>From 19th May 2022 to 30th Sept 2022: demo V2</p> <p>1st May 2022: start of the DPIA 3 if required</p> <p>From 3<sup>rd</sup> Oct 2022 to 2nd of November 2022: setup demo V3</p> <p>2nd November 2022: delivery of the DPIA 3</p> <p>From 3<sup>rd</sup> of November 2022 to August 2023: demo V3</p>
Template	InterConnect template based on CNIL.

5	Engineering Management Plan
Pilot needs and resources for security and privacy engineering	<ul style="list-style-type: none"> <li>• Anonymize the data.</li> <li>• Re-use available results and methodology from InterConnect.</li> <li>• Data to be anonymized and design the pilot accordingly.</li> <li>• No security problems if services from the InterConnect framework are being used.</li> <li>• Need an incremental agreement for data sharing.</li> <li>• Risk analysis under Excel.</li> </ul>
Engineering process	Use Engineering process from the InterConnect project.
Schedule	<p>From April 2021, the risk analysis will be started for demo 1, then the system design task and finally the implementation.</p> <p>The risk analysis will be refined for demo 2 and demo 3.</p>

6 Citizen Management Plan	
Pilot needs and resources for management	<p>Different scales for the citizen engagement need:</p> <ol style="list-style-type: none"> <li>1. Public information meetings to prepare for the involvement of users in TPM, with local partners (municipalities, associations).</li> <li>2. Participation of a sample of citizens to test the solutions (to see if there is an evolution of the solution as InterConnect is based on users).</li> <li>3. Survey (before, during, after).</li> </ol> <p>Organize focus groups before the beginning of the pilot, to work on the representations towards the EMS, to compare the results with those who worked on the pilot.</p> <p>4. Propose a support throughout the pilot, proposed by Engie and ThermoVault, we propose a collective dynamic online. (social network dedicated to the experimentation) Or also off-line: workshops, exchanges of practices between participants.</p> <p>The citizens consent to share their personal data in the context of the demonstration of InterConnect WP7.7. In exchange the InterConnect WP7.7 pilot will propose use case to maximize the renewable energies and to pilot his devices with the dynamic tariff.</p> <p>Access to Linky data requires a consent from the customer to share his data. Other data exchanged by the actors will be anonymized.</p>
Management process	<p>Specify the interaction process. For instance, needs for consent vs legitimate interest.</p> <p>Specify the engagement process, for instance:</p> <p>Information of users; Example: Are the citizen aware of security and privacy issues when using applications. Are they willing to know more about it in a simple way and not reading specifications such as GDPR? Do we have tools to easily help them to understand those issues?</p> <p>Citizen consultation.</p> <p>Transparency: Describe the process for PII principals to access their data; Describe the process for users to send review and request about the application.</p> <p>All of engagement process are linked to RGPD, as for any data collection,</p> <p>Precaution of usage in the questionnaire.</p> <p>Pilot participants are clearly informed in the consent on form on the amount and nature of shared data, as well as their purpose.</p> <p>The community member will be informed about the shared data and its purpose to confirm/reject data exchange.</p> <p>Participants get feedback via the app and can overrule settings. A contact person is assigned. Experiment feedback is given a regular interval.</p> <p>Propose community tools. Create a collective dynamic on a community network (to be decided).</p> <p>Information provided by Toulon Provence Méditerranée and the city hall of Le Pradet, based on the communication provided by the WP10 companies (InterConnect).</p> <p>Citizen consultation with the partners, TPM, and town-hall of le Pradet.</p> <p>ENGIE, ThermoVault, Trialog provide the applicative system to monitor the personal data. To send review and request about the application.</p> <p>Linky's Data: For residential customers, the regulatory requirements, and recommendations of the "Commission Nationale Informatique et Libertés" regarding consent apply. This is an essential step that the players must take. Enedis supports them and provides them with an authorization model. Each service provider will ask for the customer's consent when signing the contract.</p>
Schedule	<p>From April 2021 until September 2021: potential participants' engagement.</p> <p>From September 2021 to September 2023: participation of participants and creation of a collective dynamic.</p> <p>M48: results of user surveys. Linky's data Consent collected with each contract that is signed.</p>

## ANNEX 2.5 PORTUGUESE PILOT SPP

1 SECURITY AND PRIVACY PLAN CONTEXT	
PILOT NAME	PORTUGUESE PILOT
SUMMARY	<u>Scope and objectives:</u>

	<ul style="list-style-type: none"> <li>• This pilot is focused on enabling flexibility, not only in private residence but also in commercial buildings. The following High-Level Use Cases (HLUC) have been identified:</li> <li>• Monitor energy consumption</li> <li>• Subscription of services for domestic energy management</li> <li>• Data sharing via consumer enabled preferences and profiling</li> <li>• DSO Open Data 4 Consumer &amp; Market</li> <li>• Flexibility Aggregation of Commercial Buildings</li> <li>• Convenient Smart EV charging at Commercial Buildings</li> <li>• Enabling P2P flexibility sharing within renewable energy community via Blockchain enablers for SAREF services</li> <li>• Flexibility Management for distribution grid support</li> </ul> <p>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</p>
DESCRIPTION	<div data-bbox="418 645 1399 1184"> </div> <p><b>FIGURE 37: OVERVIEW ARCHITECTURE OF PORTUGUESE PILOT</b></p> <p>Services and Business use cases requirements and description:</p> <ul style="list-style-type: none"> <li>• Energy efficiency as a Service-Commercial/Residential:       <ul style="list-style-type: none"> <li>◦ Description: Integrated Energy Management System (iEMS) at tertiary buildings, EE enabler and flexibility aggregation.</li> <li>◦ Requirements:           <ul style="list-style-type: none"> <li>▪ Integration of diverse technology for optimal energy management / maximization of RES penetration / cost reduction.</li> <li>▪ Active and remote control over stores/buildings to enable flexibility exploitation.</li> </ul> </li> <li>◦ HLUC:           <ul style="list-style-type: none"> <li>▪ Flexibility Management for distribution grid support.</li> <li>▪ Enabling P2P flexibility sharing within renewable energy community via Blockchain enablers for SAREF services.</li> <li>▪ Flexibility Aggregation of Commercial Buildings.</li> </ul> </li> </ul> </li> <li>• Monitoring energy consumption:       <ul style="list-style-type: none"> <li>◦ Description: Throughout technological solutions, such as the Energy Management System (EMS).</li> <li>◦ Requirements:           <ul style="list-style-type: none"> <li>▪ Have immediate access to the data generated from all their appliances.</li> <li>▪ Customize some parameter related to energy consumption.</li> <li>▪ Have notifications about improvements of their consumption behaviour.</li> <li>▪ Have control based on informed decision.</li> </ul> </li> <li>◦ HLUC: Monitor energy consumption.</li> </ul> </li> <li>• Energy as a Service:       <ul style="list-style-type: none"> <li>◦ Description: The end user can have the ability to select which services to subscribe to technological solutions.</li> <li>◦ Requirements:           <ul style="list-style-type: none"> <li>▪ Forecasting.</li> <li>▪ Schedule.</li> <li>▪ Recommendation.</li> </ul> </li> <li>◦ HLUC:           <ul style="list-style-type: none"> <li>▪ Data sharing via consumer enabled preferences and profiling.</li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>DSO Open Data 4 Consumer &amp; Mar.</li> <li>Convenient Smart EV charging: <ul style="list-style-type: none"> <li>Description: Convenient EV charging with small impact in daily routine.</li> <li>Requirements: <ul style="list-style-type: none"> <li>Take advantage of the ecosystem interoperability to enable smart and convenient charging.</li> <li>Commercial customers can conveniently charge their EV's.</li> </ul> </li> <li>HLUC: Convenient Smart EV charging at Commercial Buildings.</li> </ul> </li> <li>Profiling based user data sharing: <ul style="list-style-type: none"> <li>Description: Enabling consumer data and metadata share via consumer profiling. Ingesting consumer data by matching target profiles to enable advanced third-party analytic service.</li> <li>Requirements: <ul style="list-style-type: none"> <li>Consumer data and metadata are made available by consumer proactivity.</li> <li>Consumer profiles are established.</li> <li>Consumers allows or restrict data granularity or quality.</li> <li>Different privacy techniques are employed.</li> </ul> </li> <li>HLUC: <ul style="list-style-type: none"> <li>Subscription of services for domestic energy management.</li> <li>Data sharing via consumer enabled preferences and profiling.</li> </ul> </li> </ul> </li> </ul>
--	--

2 GOVERNANCE MANAGEMENT PLAN		
Rules and legislation	<p>In Portugal the GDPR was adopted.</p> <p>Regarding the specific Portuguese legal and regulatory framework, the public policy strategy has been to increase the level of consumer flexibility and to make flexibility more relevant in terms of grid management. On the one hand, the Portuguese regulator has developed two pilot projects, in 2018 and 2019: one pilot had the goal of improving the network access tariff structure, which leads to a more effective benefit associated to demand-shifting, while the other involved consumption in providing ancillary services (tertiary reserve). Although this pilot was focused on flexibility at generation markets level, it is a clear sign towards involving customers in the sector's management decisions. On the other hand, the Portuguese government published a new self-consumption regime (Decree-Law 162/2019, Diário da República, 2019), both individual and collective, and which already opens the door to Renewable Energy Communities (RECs).</p> <p>The first self-consumption regime was published by the Decree-Law 153/2014, and it established a payment of part of the energy policy costs (the so-called "CIEG"). However, this piece of legislation did not involve the payment of any network costs by self-consumers, apart from the network costs paid due to their consumption from the grid. The current self-consumption regime was published in 2019. It establishes some rules for individual and collective self-consumption, and for renewable energy communities. The self-consumption code, published by ERSE in 2020, specified the rules for individual and collective self-consumption. The current framework establishes that only self-consumption using the grids should pay network and policy costs. There is also the possibility that the government exempts self-consumption through the grids from policy costs.</p>	
International Standards	SAREF CIM	
2.1	GOVERNANCE BODY	
Information Security Manager	Pilot preparation is in an initial phase. This item will be defined further on.	
Data Protection Officer	Pilot preparation is in an initial phase. This item will be defined further on.	
Other roles	Pilot preparation is in an initial phase. This item will be defined further on.	
Ecosystem consideration	Pilot preparation is in an initial phase. This item will be defined further on.	
2.2	ORGANISATION RESPONSIBILITY	
Entity 1	Entity Name	E-REDES
	Role	Distribution System Operator
	Address	Rua Camilo Castelo Branco, Nº 43 1050-044 Lisboa



	Contact(s)	João Falcão : <a href="mailto:joao.falcao@e-redes.pt">joao.falcao@e-redes.pt</a>
	Entity Type	Distribution System Operator
Entity 2	Entity Name	ELERGONE (SONAE)
	Role	Retailer / aggregator / energy service provider / mobility service provider
	Address	Rua de Almeiriga, nº 586, 4450-608 Leça da Palmeira
	Contact(s)	Amândio Ferreira: <a href="mailto:amandio.ferreira@elergone.pt">amandio.ferreira@elergone.pt</a>
	Entity Type	Retailer / aggregator / energy service provider / mobility service provider
Entity 3	Entity Name	INESC TEC
	Role	R&D; Coordinator of InterConnect
	Address	INESC TEC Campus da FEUP Rua Dr Roberto Frias 4200-465 Porto Portugal
	Contact(s)	David Rua: <a href="mailto:david.e.rua@inesctec.pt">david.e.rua@inesctec.pt</a>
	Entity Type	R&D
Structure of responsibility		The structure of responsibility between organization for security and privacy purposes is formed by the rules of the Grant Agreement.
2.3	Rules and procedure	
Meetings	Regular Pilot meetings (monthly) and General Assembly meetings (yearly).	
Nomination	Agreement among the responsible entities.	
Publication of minutes	Minutes and presentations available after the meetings to the consortium of the project.	
2.4	Continual improvement and periodic update	
Meetings	The meetings are called on demand in case of an incident or a proposal for improvement by a responsible entity.	
Evaluation procedure	Evaluation will take place after the 3rd workshop (where security and privacy analysis are carried out)	

3	DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.		
3.1	Pilot needs and resources for security and privacy data management	
Ownership of data	Customers, E-REDES (own dataset); ELERGONE (SONAE) (own dataset); INESC TEC (datasets)	
PII Controller	E-REDES: ELERGONE (SONAE): INESC TEC:  Pilot preparation is in an initial phase. This item will be defined further on.	
PII Processors	E-REDES: ELERGONE (SONAE): INESC TEC:  Pilot preparation is in an initial phase. This item will be defined further on.	
PII Principals	E-REDES: ELERGONE (SONAE): INESC TEC:	

		Pilot preparation is in an initial phase. This item will be defined further on.
3.2	Data Management Process	
3.2.1	Agreements	
Agreement approach		<p>The PII Controller with the consent of the PII Principal anonymizes the dataset from the smart-meter and the dataset from the sensors of the house (if any) before providing it to 3rd parties for processing.</p> <p>An agreement between the PII Controller and a 3rd party that acts as a Data Processor dictates the terms under which the data sharing between these two entities takes place.</p>
Agreement 1	Organizations	To be specified.
	Agreement template	<p>Agreement:</p> <p>Grant Agreement</p> <p>Terms and Conditions for Data Access (Agreement between data suppliers and data processors).</p>
3.2.2	Data description	
Data	Dates for collection	From Q4 2021 to Q3 2023.
	Identification of data	<p>Energy Data</p> <ul style="list-style-type: none"> <li>Whole home energy consumption (smart meter).</li> <li>Appliance/Device energy consumption (HEMS).</li> <li>Commercial Stores energy systems (BMS).</li> <li>EV chargers (BMS).</li> </ul> <p>Sensors Data</p> <ul style="list-style-type: none"> <li>Temperature, humidity, and CO2.</li> <li>Operational variables from commercial stores systems (Cooling, HVAC, lighting, PV, EV charger).</li> </ul>
	Type of data	<ul style="list-style-type: none"> <li>Household data related to energy consumption and home environment.</li> <li>Commercial buildings data related to energy consumption and home environment.</li> <li>EV charger's data related to energy consumption and home environment.</li> </ul>
	Life Cycle	<ul style="list-style-type: none"> <li>Energy Data is generated periodically.</li> <li>Sensor Data is generated on sensors' status change.</li> <li>Data is stored in the cloud without any expiration/deletion date.</li> <li>In commercial buildings, the data is stored locally in the BEMS system. Data is logged every 15 minutes and stored for a period of 1 year (configurable).</li> </ul>
	Data description	InterConnect Deliverable D1.3 (at this moment).
3.2.3	Data exchange	
Data flow		InterConnect Deliverable D1.3
Data access control chart		InterConnect Deliverable D1.3
3.2.4	Data access monitoring	
Data access verification procedure		Each Data Supplier provides/revokes access to data manually and explicitly to a Data Consumer/Processor.
3.2.5	Data Registry	
Registry of agreements		<p>Project's drive (digital)</p> <p>Companies' headquarters (paper)</p>
Registry of data sets		Project's drive (digital)
Registry of citizen consents		Consumers provide their written consent by agreeing in terms and conditions before being included in the Portuguese Pilot.

<b>4</b>	<b>Risk Management Plan</b>
<b>4.1</b>	<b>Pilot needs and resources for security and privacy risk management</b>
Context for privacy analysis	<p>All the use cases in the pilot that uses user information will use anonymized data. The data processors identify the different datasets by a home-id and they are not aware of the home's exact location or other personal information.</p> <p>The information that connects the home-ids with the location and the identification of the resident is only known to the Data Suppliers.</p> <p>The EV-Charger user's personal data will be also anonymized.</p> <p>The commercial buildings will not use personal data.</p>
Context for security analysis	<p>The datasets are anonymized, and they are not for open access. The access will be given only to entities/persons with a clear justification.</p> <p>Data transfer should be encrypted from the devices, through the cloud database to the Data Processor.</p> <p>Authentication/Authorization mechanisms should prevent any data breach in the database.</p>
Context for the project	It will be used security and privacy mechanisms supplied by the Consortium, by design, in the Interoperability layer, and in the P2P blockchain technologies.
<b>4.2</b>	<b>Risk management process</b>
<b>4.2.1</b>	<b>Security</b>
Methodology	To be specified.
Schedule	Pilot preparation is in an initial phase. This item will be defined further on.
Template	Pilot preparation is in an initial phase. This item will be defined further on.
<b>4.2.2</b>	<b>Privacy</b>
Methodology	To be specified.
Schedule	Pilot preparation is in an initial phase. This item will be defined further on.
Template	Pilot preparation is in an initial phase. This item will be defined further on.

<b>5</b>	<b>Engineering Management Plan</b>
Pilot needs and resources for security and privacy engineering	Will be adopted the access control mechanism that will be provided by the Interoperability framework of InterConnect.
Engineering process	<p>NIST Frameworks (Security and Privacy)</p> <p>ISO/IEC 27550 - privacy engineering guidelines</p> <p>ISO/IEC 27001 - requirements for an information security management system</p> <p>ISO/IEC 27701 - requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System</p>
Schedule	Pilot preparation is in an initial phase. This item will be defined further on.

<b>6</b>	<b>Citizen Management Plan</b>
Pilot needs and resources for management	<p>Users need to provide their consent to the Data Controllers.</p> <p>Users need to provide their consent to the Data Processors.</p>

Management process	<p>Data Controllers that are also responsible for the hardware installation of the various sensing devices in the house, receive the user's consent before the installation.</p> <p>Users can monitor their house environment and energy consumption, while Data Controllers are able to process their data and offer services to the users (dashboards, remote control/monitoring, etc.).</p> <p>Moreover, Data Controller can provide their data (anonymized) to 3rd parties to provide advanced services to the users as an exchange (data analytics, recommendations etc.).</p> <p>In the context of the pilot's use cases, users will be asked to use a mobile application developed by a Data Processor. Once the user opens the application, he will be informed about the usage of his/her data and provide his/her consent to proceed.</p>
Schedule	<p>Consent from the users regarding the Data Controllers will be given.</p> <p>Consent from the users regarding the mobile applications and their data processing will be given at the time the user opens the application.</p>

## ANNEX 2.6 ITALIAN PILOT SPP

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	Italian Piloting activities @ Merezzate REDO social dwellings
SUMMARY	<p>The Italian Piloting activities intends to pursue end users an enhanced monitor and capability control of home connected devices. The single end users will be provided with energy management options to optimize their costs by rescheduling the electrical loads (time shifting) according to the grid constraints that the DSO will provide. The aggregation and management of e loads of end users in a sort of energy community will enable the Living Serving Provider to mimic the participation in the flexibility market.</p> <p>To this end a seamless interoperability and data exchange between systems and devices within the Planet (Idea) App is to be ensured under proper provisions of data privacy and security.</p> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p><b>FIGURE 38: OVERVIEW ARCHITECTURE OF ITALIAN PILOT</b></p> <p>User schedules a cycle on a connected product to run later in the day. Cycles can be programmed either in the device App or on the product itself. Cycle information is sent by the App/Appliance to the manufacturer's cloud. The power profile of that cycle start time and end time are sent from the Manufacturer's cloud to the living service provider ones and from there to the Energy service provider platform. The Energy Service provider uses the information of power profile to update the curve of forecasted flexible load for that user, case he has provided consent for flexibility for that product, or to update the curve of non-flexible load in case flexibility is denied. Whatever is the outcome, it is then aggregated to create a curve of the total flexible/non-flexible load offered by all users. On a periodic basis (asynchronously from the cycle scheduled), the Energy Service provider receives information on the home total energy consumption from the smart meter. This information is used to validate the forecast of non-flexible load for that user. The forecast is based on historical data and the information from the smart meter is to validate it. For example, if user's home consumption is in general less than 500W/h during morning hours, this can form the baseline, but the day in which the user is at home in the morning and is using electrical devices that bring his energy consumption over 2KW/h, the</p>

	<p>baseline cannot be used a new value is to be used as a reference. The Energy service provider periodically reports the two aggregated power curves, flexible and non-flexible loads, to the Living service provider who reports them to the Aggregator. The Aggregator examines the two forecasts and assesses if there are opportunities to offer energy flexibility to the energy market or if there are other opportunities to make spot offers to modify the forecasted power consumption. The aggregator provides to the living service provider the required new curves (flexible load and/or total load) together with the overall remuneration if they are achieved the living service provider sends the request to the energy service provider to identify to which users should be involved for the automatic load shifting or sending notifications about spot offers to reduce/increase energy consumption. The energy service provider defines which users must be involved and send the request for load shifting or notifications to Living service provider. The Living service provider sends the request to the manufacturer's platform. The manufacturer's platform updates the cycle's information to the new time and updates the App or directly the product. The new timing will be reflected in the EM App as when a new cycle is scheduled. The Living service provider sends notifications to the users on the EM App to alert about spot offers.</p> <p>These are the PUCs implemented in the pilot:</p> <p>PUC1 - Provide consent to data transfer</p> <p>End User provides consent to the Manufacturer to share data about specific devices with Energy Manager.</p> <p>Device pairing to foster a seamless data flow and collection thus enabling management and control capability at granular level</p> <p>PUC2 -Enable flexibility programme</p> <p>User provides general consent to flexibility for certain products. The consensus may be revoked specifically for a product in a certain day. Scheduled cycles can then be shifted by EM within limits set by user</p> <p>PUC3 - exchange of aggregated flexibility data</p> <p>Information exchange between the Aggregator and the Energy service provider.</p> <p>In this use case the Aggregator offers ancillary services to the TSO (not present in Italian Pilot) by using the energy flexibility of an aggregate of residential users. If the service is carried out, the Aggregator provides a remuneration to the users who effectively have participated.</p> <p>PUC4 - Time of use tariffs</p> <p>This Use Case provides an incentive-based remuneration mechanism for load shifting. To this end the DSO, interacting with the ESP will provide the Aggregator with dynamic energy prices over time. The scheduled time framed prices tables will be pursued to the Living Service Provider to trigger power requests modulated by Energy Management algorithms capabilities to the end users. The EM will schedule and manage through the app the connected smart devices within their flexibility capabilities to optimize the power consumption and voltage levels according to the time of use tariffs.</p> <p>PUC5 - Awareness and notification</p> <p>This use case describes the functionality of sending notifications to the end users through the Planet App to engage them to be part of an energy community unlock benefits and perks whether EM rescheduling of electrical loads tips are met.</p> <p>End User receives alerts and notifications about:</p> <ul style="list-style-type: none"> <li>• Remuneration status for the flexibility granted</li> <li>• Information about incentives from Aggregator and timing</li> <li>• Status of connected devices</li> <li>• Load forecasting</li> <li>• Benchmark based on historical data analysis</li> </ul>
--	---

2 GOVERNANCE MANAGEMENT PLAN	
Rules and legislation	Planet Smart City applies the requirements of the EU GDPR as a minimum standard for data protection in all jurisdictions in which we operate. We apply local legal and regulatory requirements (e.g., Brazil LGPD) where compliance with GDPR would violate the organisation's legal obligations.
International Standards	NIST
2.1 GOVERNANCE BODY	
Information Security Manager	To be specified.

Data Protection Officer		The DPO of Planet Smart City is Robert Healey ( <a href="mailto:robert.healey@formiti.com">robert.healey@formiti.com</a> ).
Other roles		Alex Leathard (Head of Data & Insights, Planet Smart City) Rafael Tella (General Counsel, Planet Smart City)
Ecosystem consideration		To be specified.
2.2	ORGANISATION RESPONSIBILITY	
Entity 1	Entity Name	Planet Holding Ltd
	Role	Controller
	Address	2nd Floor 22 Eastcheap, London, England, EC3M 1EU
	Contact(s)	Robert Healey ( <a href="mailto:robert.healey@formiti.com">robert.healey@formiti.com</a> )
	Entity Type	Private limited
Structure of responsibility		Robert Healey will sign off on all data protection and privacy matters.
2.3	Rules and procedure	
Meetings		The governance body meets on an ad-hoc basis as required by the needs of the organisation.
Nomination		There is currently no nomination procedure for the governance body.
Publication of minutes		The minutes of governance body meetings will be published via Microsoft SharePoint.
2.4	Continual improvement and periodic update	
Meetings		The governance body meets on an ad-hoc basis, as dictated by the needs of the organisation, and in response to data incidents. Continual Improvement meetings are conducted on an annual basis by means of presentation to the Senior Leadership Team (SLT).
Evaluation procedure		The DPO performs an annual Privacy Maturity Assessment according to the GAPP. The results of the assessment are reported to the SLT and used to create a remediation plan. The Head of Data & Insights performs an annual Data Management Maturity assessment according to the principles of the CMMI. The results of the assessment are reported to the SLT and used to create a remediation plan. The Head of IT performs an annual assessment of the technology infrastructure and cybersecurity. The results of the assessment are reported to the SLT and used to create a remediation plan.

3		DATA MANAGEMENT PLAN	
InterConnect data management plan is the first input.			
3.1		Pilot needs and resources for security and privacy data management	
Ownership of data		To be specified.	
PII Controller		To be specified.	
PII Processors		To be specified.	
PII Principals		To be specified.	
3.2		Data Management Process	
3.2.1		Agreements	
Agreement approach		Parties to enter into Data Protection Addendum or Data Sharing Agreements and to rely on Legitimate Interest and on the performance of Contracts, as the lawful basis for the processing of PII.	
Agreement Item 1	Organizations	CWS	



	Agreement template	Data Sharing Agreement template in project's repository.
Agreement 2	Organizations	RSE
	Agreement template	Data Sharing Agreement template in project's repository.
Agreement 3	Organizations	WattsDat
	Agreement template	Data Sharing Agreement template in project's repository.
Agreement 4	Organizations	Whirlpool
	Agreement template	Data Sharing Agreement template in project's repository.
3.2.2 Data description		
Data 1	Dates for collection	The data journey begins when the customer downloads and registers in the Planet App.
	Identification of data	The data is recorded identifying data Subject categories, and by categories of data types.
	Type of data	<ul style="list-style-type: none"> <li>Personal data will be any data that can identify a living person or be used in connection with other data to identify a living person, this includes business data example business email address</li> <li>Business data equals statistical data that cannot be used to identify a living person</li> <li>Data transferred from IoT and smart meter devices that do not carry personal data but is needed to provide the service.</li> </ul>
	Life Cycle	<ul style="list-style-type: none"> <li>Storage time defined by the pilot retention schedule.</li> <li>Deletion process will be in line with the data retention schedule for the pilot.</li> </ul>
	Data description	IOT Identifier information.
Data 2	Dates for collection	The data journey begins when users agree to participate in the project. From this moment on, the exchange of information with Whirlpool, RSE and Wattsdat begins.
	Identification of data	The data is recorded identifying data Subject categories, and by categories of data types.
	Type of data	<ul style="list-style-type: none"> <li>Personal data will be any data that can identify a living person or be used in connection with other data to identify a living person, this includes business data example business email address.</li> <li>Business data equals statistical data that cannot be used to identify a living person.</li> <li>Data transferred from IoT and smart meter devices that do not carry personal data but is needed to provide the service.</li> <li>Storage time defined by the pilot retention schedule.</li> <li>Deletion process will be in line with the data retention schedule for the pilot.</li> </ul>
	Life Cycle	<ul style="list-style-type: none"> <li>Storage time defined by the pilot retention schedule.</li> <li>Deletion process will be in line with the data retention schedule for the pilot.</li> </ul>
	Data description	IOT Identifier information
3.2.3 Data exchange		
Data flow		There will be flows from the entities, Whirlpool to the interoperability layer, Wattsdat to the interoperability layer, RSE aggregator data to the interoperability layer. A bidirectional feed between the Planet APP and the interoperability layer. Please see data mapping and privacy document.
Data access control chart		The data access chart for employees and entities involved in the pilot will be as follows:

		<table><tr><th></th><th>PLANET</th><th>WHIRPOOL</th><th>RSE</th><th>WATTS DAT</th></tr><tr><td>USER INFORMATION</td><td>R/W</td><td>R/W</td><td></td><td></td></tr><tr><td>USER ID</td><td>R/W</td><td>R/W</td><td>R</td><td></td></tr><tr><td>USER DEVICES</td><td>R</td><td>R/W</td><td>R</td><td></td></tr><tr><td>DEVICE IDS</td><td>R</td><td>R/W</td><td>R</td><td>R</td></tr><tr><td>DEVICE SCHEDULING</td><td>R/W</td><td>R/W</td><td>R</td><td>R</td></tr></table>		PLANET	WHIRPOOL	RSE	WATTS DAT	USER INFORMATION	R/W	R/W			USER ID	R/W	R/W	R		USER DEVICES	R	R/W	R		DEVICE IDS	R	R/W	R	R	DEVICE SCHEDULING	R/W	R/W	R	R
	PLANET	WHIRPOOL	RSE	WATTS DAT																												
USER INFORMATION	R/W	R/W																														
USER ID	R/W	R/W	R																													
USER DEVICES	R	R/W	R																													
DEVICE IDS	R	R/W	R	R																												
DEVICE SCHEDULING	R/W	R/W	R	R																												
3.2.4	Data access monitoring																															
Data access verification procedure	<p>Planet App operates a Role-Based Access Control mechanism wherein users of the app (both employees of Planet and customers) are assigned a role on account creation (the identity of which is stored in the Planet App database), and the assigned role is granted specific privileges, e.g., customers are by default assigned a user role that is granted sufficient privileges to access data associated with the logged-in user only, cannot post news items to districts, etc.</p> <p>Elevated privileges are available to a very small number of named individuals within Planet. It is not possible to obtain elevated privileges via the Planet App mobile app.</p> <p>Integrations with social logins are implemented via OAuth2. OAuth tokens have a finite lifetime within Planet App.</p> <p>Planet's data warehouse integration has read-only permission to extract business information from Planet App for downstream analytics. User IDs are used to process data pseudo-anonymously; personal data are either excluded from processing or securely hashed prior to analysis.</p>																															
3.2.5	Data Registry																															
Registry of agreements	Agreements are stored and managed via an InterConnect-specific segregation of our compliance platform (Formiti365).																															
Registry of data sets	<p>Planet App stores the following datasets in an Azure database for PostgreSQL Server instance:</p> <ul style="list-style-type: none"><li>User account information (First Name, Last Name, email, phone, mobile phone, tax code, vat code, date of birth, district to which it belongs, flat number, address).</li></ul> <p>Planet App stores the following datasets in Azure CosmosDB:</p> <ul style="list-style-type: none"><li>Raw IoT device message content.</li><li>Planet App stores the following dataset in Azure SQL;</li><li>Aggregated IoT device data content.</li><li>Planet App stores the following dataset in Azure Blob Storage;</li><li>User documents and photos and others files.</li></ul> <p>Planet App stores the following datasets in Snowflake:</p> <ul style="list-style-type: none"><li>All datasets from the Planet App SQL Server, excluding OAuth tokens and PII.</li></ul>																															
Registry of citizen consents	Planet App requires customers to accept a privacy policy on account creation. We intend to add new functionality to store and manage user consents.																															

4	Risk Management Plan	
4.1	Pilot needs and resources for security and privacy risk management	
Context for privacy analysis	Planet Smart City will complete a DPIA, which will focus on the data transfers and encryption levels deployed to protect the data at rest and in transit.	
Context for security analysis	A security analysis will need to be carried out on the security of the API deployed to allow for the data to be transferred to and from the InterConnect interoperability layer.	
Context for the project	The pilot will utilise the interoperability data layer project expertise of the Consortium.	
4.2	Risk management process	
4.2.1	Security	
Methodology	<p>STRIDE</p> <ul style="list-style-type: none"> <li>Security Properties: Authentication, Integrity, Non-Repudiation, Confidentiality, Availability, Authorization.</li> <li>Security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.</li> </ul>	

	NIST Security Framework (e.g., Identify, Protect, Detect, Respond, and Recover).
Schedule	Each pilot will schedule meeting 3 (focusing on security and privacy risk analysis).
Template	ISO/IEC 27005. This section will be elaborated in WP5 to describe the action plan set up to support the pilots and reports on the result of the security and risk analysis, the requirements for mitigation and the analysis of compliance readiness.
4.2.2	Privacy
Methodology	To be specified.
Schedule	Each pilot will schedule meeting 3 (focusing on security and privacy risk analysis).
Template	ISO/IEC 29134. This section will be elaborated in WP5 to describe the action plan set up to support the pilots and reports on the result of the security and risk analysis, the requirements for mitigation and the analysis of compliance readiness.

5	Engineering Management Plan
Pilot needs and resources for security and privacy engineering	<p>Planet Smart City will leverage the following security and privacy capabilities, competences and persons that already exists in the organisation:</p> <p>Capabilities:</p> <ul style="list-style-type: none"> <li>• CWS (product development consultancy).</li> <li>• Planet Smart City Data &amp; Insights function.</li> <li>• Planet Smart City IT function.</li> </ul> <p>Competences:</p> <ul style="list-style-type: none"> <li>• Cybersecurity.</li> <li>• Data engineering.</li> <li>• Data privacy.</li> <li>• Data protection.</li> <li>• Privacy engineering.</li> <li>• Security architecture.</li> <li>• Technical documentation.</li> </ul> <p>Persons:</p> <ul style="list-style-type: none"> <li>• DPO;</li> <li>• CTO (CWS);</li> <li>• CWS software engineers;</li> <li>• Head of IT;</li> <li>• Head of Data &amp; Insights;</li> <li>• Planet Smart City data engineers;</li> </ul> <p>The pilot will make use of the Planet App as a central point of access for customers. This solution includes identity management and RBAC. The pilot will also make use of the InterConnect interoperability layer to send and receive data between parties.</p>
Engineering process	<p>Engineering: Planet Smart City and CWS follow a lightweight implementation of the SDLC in the SCRUM mould.</p> <p>Security engineering: Planet Smart City broadly implements the NIST Framework.</p> <p>Privacy engineering: e.g., Planet Smart City broadly implements the NIST Privacy Framework.</p>
Schedule	<p>Piloting activities under WP7 provisions formally started in October 2020, lasting till the end of the InterConnect project, foreseen in September 2023. The roll out of the Italian Pilot will meet end user engagement and active participation targeting summer 2021. At that date, with the delivery of white goods to early adopters, pilot's implementation and data flow will finally take place.</p> <p>Common Digital reference architectures, ontologies, communication standards definition, in addition to interoperability layer deployment, and delivery of adapters by WP5 activities will be ensured earliest during April 2021 to come to a final digital setup by October 2021.</p> <p>Agreement between pilot partners, namely Whirlpool, RSE, and Planet are, at the time being (M18), still work in progress but Data sharing agreement and Data protection addendum have been already proposed in addition to the early definition of the relationship between Planet and end users which will possibly state:</p> <ul style="list-style-type: none"> <li>• The beneficiaries must be clearly informed of the subject of the experimentation activities and the obligations involved</li> </ul>

	<ul style="list-style-type: none"> <li>The contract between the parties must make explicit the efficiency of the device to be delivered</li> <li>The use of the device through the project may be necessary in certain time slots. The users shall take note of the tariffs associated with the use of energy for those specific time slots and of the related costs. No additional charges shall be paid by Planet in the event of the devices being used at higher cost times.</li> </ul> <p>It has not yet been discussed nor defined a risk analysis which will follow the instantiation of mutual agreement between all the participating parties, possibly during Positioning meeting 3 (security and privacy risk analysis).</p>
--	---

6	Citizen Management Plan
Pilot needs and resources for management	Citizen engagement will be agreed together with the Real Estate developer and the Social Housing Foundation (FHS) operating in the Merezate REDO district where the piloting activities will take place.
Management process	<p>Information material has been realized within the scope of InterConnect WP10 activities, counting on a promotional video and an informative leaflet. These materials contain references to security and privacy issues. Information material will be let available to end users once the purchasing activities will be agreed, targeting 2021.</p> <p>Interested citizens and the ones selected for piloting activities will need to register to the program. Contracts to define roles, mutual responsibilities and of course Data related issues will be signed among the consortium and the end users themselves.</p> <p>In case of questions related to the processing of personal data or to the exercise of your rights end users can contact our Data Protection Officer through the email dpo@inesctec.pt</p> <p>The personal data collected by answering this registration will be used by INESC TEC, as leader of the InterConnect project, and Planet Smart City, as leader of the Italian pilot. Anonymized data can be passed to other partners in the consortium for research purposes. The data will be deleted six months after the end of the project.</p>
Schedule	User engagement is scheduled to be started during the 3rd quarter of 2021; the purchase of connected devices will be accomplished by the end of 2021. It may be possible to have an early adopters pool of end users to start the piloting of activities by June 2021, according to the deployments of digital solution for energy and to the delivery of connected white goods.

## ANNEX 2.7 CROSS-BORDER INTEROPERABILITY PILOT SPP

This pilot is enclosed within task 7.8 Overarching demonstration. It is not a specific piloting in a specific country, it aims to demonstrate the interoperability advantages between the digital platforms operating in several of the national pilots. The demonstration will be shown by using a service that enables the flexibility information exchange in cross-border.

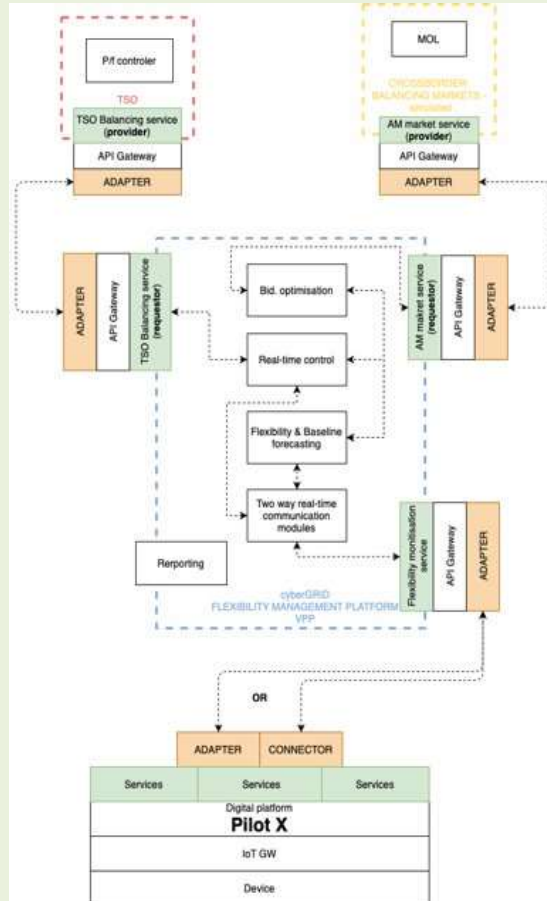
1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	Cross-border interoperability by cyberGRID
SUMMARY	This pilot encompassed in Task 7.8 will demonstrate the interoperability advantages between the digital platforms operating in several of the national pilots by creating an overarching demonstration.
DESCRIPTION	<p>The focus of the demonstration will be to showcase the functionalities of using a service that enable exchanging flexibility information cross-border.</p> <p>To demonstrate cross-border interoperability, flex services can be offered to a market player, in this case a (simulated) TSO.</p> <p>Ancillary services will be offered to on aFRR and mFRR markets by aggregation of geographically distributed flexibility resources like loads, renewables, and storage.</p>

The graphic below illustrates the offered service: Flexibility monetisation

Southern-bound services (to be requested):

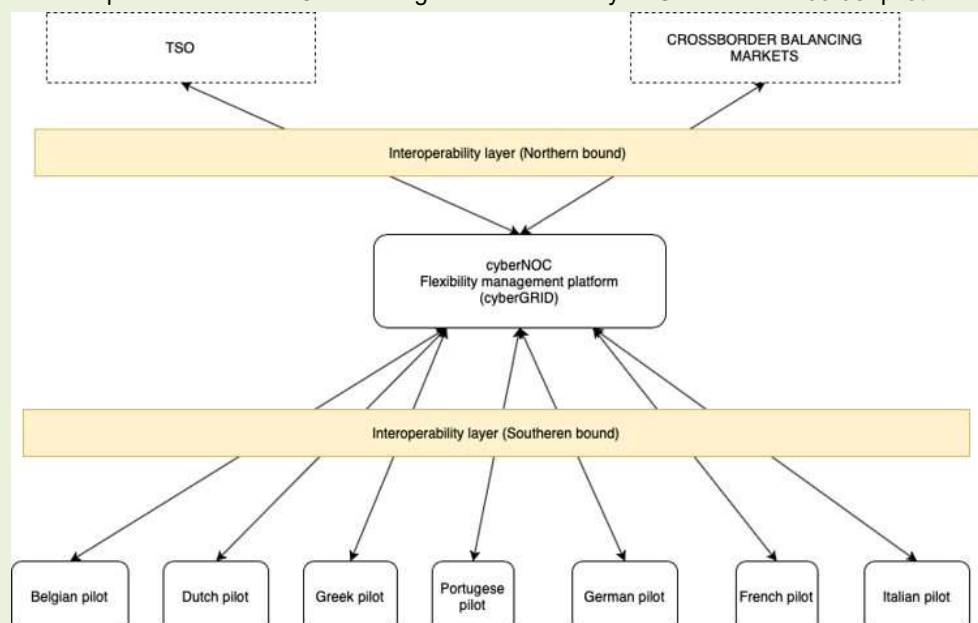
Flexibility service (energy assets that can offer flexibility to be utilised and monetised).

Northern-bound services: TSO Balancing service, Ancillary market service



**FIGURE 39: OVERVIEW ARCHITECTURE OF CROSS-BORDER PILOT**

Here is a simplified view of the Overarching Architecture of cyberGRID's cross-border pilot:



**FIGURE 40 SIMPLIFIED OVERVIEW OF THE CROSS-BORDER PILOT**

<b>2</b>	<b>GOVERNANCE MANAGEMENT PLAN</b>	
Rules and legislation	GDPR	
International Standards	To be specified.	
<b>2.1</b>	<b>GOVERNANCE BODY</b>	
Information Security Manager	Andraz Andolsek, Head of Software Development	
Data Protection Officer	Data of individual persons will be anonymized	
Other roles	To be specified.	
Ecosystem consideration	To be specified.	
<b>2.2</b>	<b>ORGANISATION RESPONSIBILITY</b>	
Entity 1	Entity Name	It is anticipated that each InterConnect, country-level pilot would need to identify a main point-of-contact for (POC)the cyberGRID pilot. cyberGRID is in contact with all the country-level pilots, however, at this stage, main POCs have yet to be identified.
	Role	Pilot leader
	Address	Weimarer Straße 119/1 1190 Wien, Austria
	Contact(s)	Andraz Andolsek - <a href="mailto:andraz.andolsek@cyber-grid.com">andraz.andolsek@cyber-grid.com</a>
	Entity Type	Consultancy
Structure of responsibility		<i>To be specified.</i>
<b>2.3</b>	<b>Rules and procedure</b>	
Meetings	Project rules should be applied.	
Nomination	<i>To be specified.</i>	
Publication of minutes	<i>To be specified.</i>	
<b>2.4</b>	<b>Continual improvement and periodic update</b>	
Meetings	To be specified.	
Evaluation procedure	An evaluation can take place after the 3rd workshop (where security and privacy analysis are carried out).	

### 3 DATA MANAGEMENT PLAN

The plan will be specified until the m4 meeting. As cyberGRID is not in charge of the user's data. All the data received to the cyberGRID platform will be anonymised.

### 4 RISK MANAGEMENT PLAN

The plan will be specified until the m4 meeting. As cyberGRID is not in charge of the user's data. All the data received to the cyberGRID platform will be anonymised.

### 5 ENGINEERING MANAGEMENT PLAN

The plan will be specified until the m4 meeting.

### 6 CITIZEN ENGAGEMENT PLAN

Not applicable for the pilot.



## ANNEX 2.8 GERMAN PILOTS SPP

## ANNEX 2.8.1 NORDERSTEDT LOCATION (EEBUS)

1	SECURITY AND PRIVACY PLAN CONTEXT
PILOT NAME	Residential Pilot Norderstedt (GERMAN PILOT)
SUMMARY	<p>Manage overload and underload scenarios using bi-directional communication from grid to device level via an Energy Management System (EMS). Installation of the EMS to aggregate energy demands and offers, manage flexibilities and grid commands. Demonstrate transition of mobility and heating as well as transition to renewable energy productions at no grid expansion.</p> <p><i>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</i></p>
DESCRIPTION	<p>Stadtwerke Norderstedt (SN) wants to provide all own customers with and maximize utilization of wind energy and an extension of existing power cables should be prevented or minimized even if new E-Vehicles or Heat Pump systems will be attached to the grid network. Therefore we are creating with the pilot a communication system between the houses with their intelligent devices and the DSO and Energy Provider to manage the whole energy system based on tariff information, capacity management and customer preferences. In the house there is an intelligent energy management device located with the communication channels via the BSI certified SMGW to the DSO/ESP and via cloud protocol (manufacture cloud protocol definition) to the White Goods devices companies. The other communication is in the local home network protected via TLS security.</p> <p>We will realize the following use cases:</p> <ul style="list-style-type: none"> <li>HLUC1: Maximize utilization of renewable -wind- energy @grid connection point (general generation).</li> <li>HLUC2: Maximize utilization of DER energy consumption in premises (local generation).</li> <li>HLUC3: Grid stability via power limitation at grid connection.</li> <li>HLUC4: Maximize flexible energy consumption in premises.</li> <li>HLUC5: Provide dashboard to inform user about status and stimulate to use opportunities.</li> </ul>

<b>2</b>	<b>GOVERNANCE MANAGEMENT PLAN</b>
Rules and legislation	GDPR
International Standards	ISO 15118; IEC 61851-1; VDE 2829-6 BSI-CCPP0073/TR03109

<b>2.1 GOVERNANCE BODY</b>		
Information Security Manager	Security	It must be defined together with Stadtwerke Norderstedt as DSO/ESP As pilot project responsible person: <a href="mailto:bartsch@eebus.org">bartsch@eebus.org</a> – Ullrich Bartsch
Data Protection Officer		To be specified.
Other roles		To be specified.
Ecosystem consideration		To be specified.
<b>2.2 ORGANISATION RESPONSIBILITY</b>		
Entity 1	Entity Name	EEBUS Initiative e.V.
	Role	Pilot leader
	Address	Butzweilerhof-Allee 4
	Contact(s)	50829 Köln
	Entity Type	Ulrich Bartsch: <a href="mailto:bartsch@eebus.org">bartsch@eebus.org</a>
Entity 2	Entity Name	KEO GmbH
	Role	Sub pilot leader
	Address	Butzweilerhof-Allee 4 50829 Köln
	Contact(s)	Thomas Fishedick : <a href="mailto:fishedick@keo-connectivity.de">fishedick@keo-connectivity.de</a>
	Entity Type	Company to provide the EMS in the pilot
Entity 3	Entity Name	Stadtwerke Norderstedt
	Role	Pilot creator and first level support
	Address	Heidbergstraße 101-111, 22846 Norderstedt
	Contact(s)	Thorsten Meyer: <a href="mailto:tmeyer@stadtwerke-norderstedt.de">tmeyer@stadtwerke-norderstedt.de</a>
	Entity Type	Company of City of Norderstedt for the City communication and energy supply
Structure of responsibility		Stadtwerke Norderstedt (SWNOR) is responsible part of the pilot to have the contract with the pilot user and with the companies/partner like Vaillant, Daikin, BSH, Miele, Theben, KEO, Wirelane. SWNOR provide the pilot user via information platform. Some partner from the pilot will have their own product platform with the user agreement via the company app.
<b>2.3 Rules and procedure</b>		
Meetings		Regular pilot meetings, intercompany meetings/checks, and meetings organised in consortium. In case of incidents specific meetings will be organized.
Nomination		Participation defined from the pilot partners.
Publication of minutes		Presentations and defined tasks (via e-mail, in MS teams and stored on MS SharePoint/NextCloud).
<b>2.4 Continual improvement and periodic update</b>		
Meetings		Regular pilot meetings, intercompany meetings/checks, and meetings organised in consortium. In case of incidents specific meetings will be organized.
Evaluation procedure		During pilot meetings the evaluation is possible. And after the 3rd workshop evaluation will also be done.

<b>3 DATA MANAGEMENT PLAN</b>	
InterConnect data management plan is the first input.	
<b>3.1</b>	Pilot needs and resources for security and privacy data management

Ownership of data		SWNOR will provide the data for the pilot user via desktop application together with helpful notifications.
PII Controller		SWNOR receives/collects the data from the different environments.
PII Processors		SWNOR with the backend solutions/services will process the data and reacts on it.
PII Principals		The pilot partner from Stadtwerke Norderstedt.
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach		For the Norderstedt pilot everything will be managed between the different responsible parts of SWNOR.
Agreement 1	Organizations	SWNOR together with their end customer.
	Agreement template	Contract will be created from SWNOR specially for this pilot, work in progress.
<b>3.2.2 Data description</b>		
Data 1	Dates for collection	From Q4 2021 to Q3 2023.
	Identification of data	<ol style="list-style-type: none"> <li>1. Electrical consumption of the houses.</li> <li>2. Forecast of the house.</li> <li>3. Tariff information.</li> <li>4. Power limitation.</li> <li>5. EMS process data.</li> </ol>
	Type of data	<ol style="list-style-type: none"> <li>1. Critical to service data.</li> <li>2. Business data.</li> <li>3. Business data.</li> <li>4. Critical to service data.</li> <li>5. PII (Personally Identifiable Information).</li> </ol>
	Life Cycle	No storage time/deletion process is therefore fixed at this point; Will be defined together with SWNOR.
	Data description	The data will be defined in the next SAREF4ENRER specifications for the different Use Cases.
<b>3.2.3 Data exchange</b>		
Data flow		<ol style="list-style-type: none"> <li>1. EMSE transfers the data via SMGW to the backend from SWNOR.</li> <li>2. EMS communicate with all different devices in the house.</li> <li>3. EMS provides for first level support service data for SMNOR.</li> </ol>
Data access control chart		To be done after final decision with the EMS manufacture and SWNOR.
<b>3.2.4 Data access monitoring</b>		
Data access verification procedure		<i>To be specified.</i>
<b>3.2.5 Data Registry</b>		
Registry of agreements		<i>To be specified.</i>
Registry of data sets		<i>To be specified.</i>
Registry of citizen consents		<i>To be specified.</i>

## 4 RISK MANAGEMENT PLAN

In the context of the project, this sub pilot will not use innovation capabilities from the Consortium, except for the SAREF ontology and interoperability adopters for EEBUS protocol. The plan will be specified until the m4 meeting.

5	Engineering Management Plan	
Pilot needs and resources for security and privacy engineering	To be specified within the SPOCS meeting.	
Engineering process	Project management driven within Pilot meetings.	
Schedule	Every two weeks.	

## 6 CITIZEN ENGAGEMENT PLAN

This pilot does not involve citizens. Not relevant for the project.

## ANNEX 2.8.2 HAMBURG LOCATION (KEO-CONNECTIVITY)

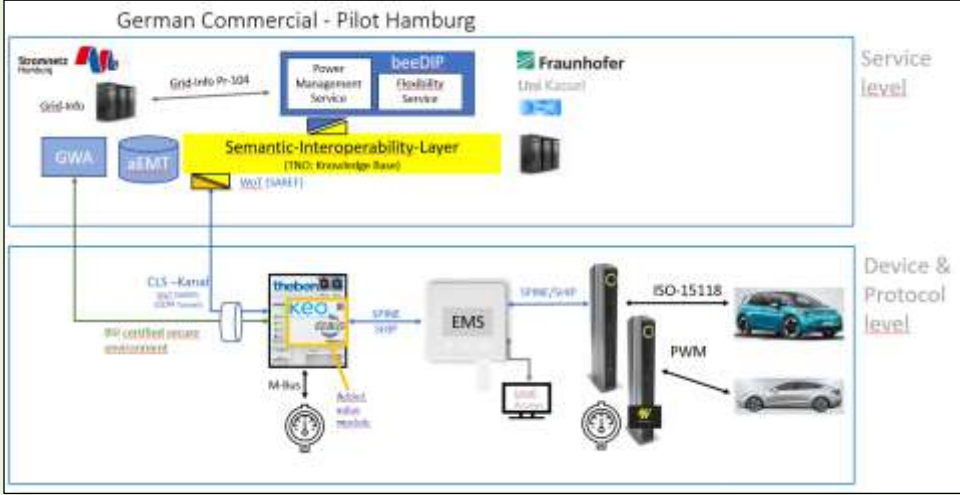
1	SECURITY AND PRIVACY PLAN CONTEXT	
PILOT NAME	Commercial Pilot Hamburg (Hotels)	
SUMMARY	<p>Installation of smart charging infrastructure at hotel location. Develop a future-oriented hotel providing grid Compatible and tariff-based charging infrastructure.</p> <p>NOTE: For more detailed information about HLUC (High Level Use Cases), see D1.3.</p>	
DESCRIPTION	<p>Wallboxes will be installed at five hotel locations. They interact with a local EMS via EEBUS communication. The EMS communicates with the SMGW via EEBUS communication, too. It gets and sends information from and to the smart grid. The EMS is realizing the local user features like overload protection and price optimized device operations.</p> <p>The SMGW uses the transparent CLS communication path to distribute the EEBUS WoT (SAREF) data to the Semantic Interoperability Layer.</p> <p>The Service Application on the beeDIP platform from Fraunhofer IEE is communicating via WoT (SAREF) with the Semantic-Interoperability-Layer, too.</p> <p>BeeDip also uses data from the smart grid with the help of the IEC 60870-5-104 (Anwendungsbezogene Norm für Fernwirkaufgaben in IP-Netzen) to realize the information for GRID Features like Power limitation and flexible tariffs, power consumption and energy forecast.</p> 	

FIGURE 42: OVERVIEW ARCHITECTURE OF GERMAN PILOT IN HAMBURG

2	GOVERNANCE MANAGEMENT PLAN	
Rules and legislation	GDPR	

International Standards		VDE_2829-6 (EEBUS); BSI-CCPP0073 / TR03109; OCPP; ISO 15118; IC 61851-1;
2.1	GOVERNANCE BODY	
Information Security Manager		Inserted by partners within next Pilot meeting OCPP: Wirelane Sahil Gambhir < <a href="mailto:sahil.gambhir@wirelane.com">sahil.gambhir@wirelane.com</a> > Application Service: Fraunhofer IEE
Data Protection Officer		To be specified.
Other roles		To be specified.
Ecosystem consideration		To be specified.
2.2	ORGANISATION RESPONSIBILITY	
Entity 1	Entity Name	KEO GmbH
	Role	Local EMS
	Address	KEO GmbH Butzweilerhof-Allee 4 50829 Cologne Germany
	Contact(s)	Marc Eulen < <a href="mailto:eulen@keo-connectivity.de">eulen@keo-connectivity.de</a> >; Michael Spall < <a href="mailto:spall@keo-connectivity.de">spall@keo-connectivity.de</a> >; Thomas Fishedick < <a href="mailto:fishedick@keo-connectivity.de">fishedick@keo-connectivity.de</a> >
	Entity Type	EEBUS Solution Stack Provider
Entity 2	Entity Name	Wirelane
	Role	Charge Point Operator
	Address	Prinzregentenplatz 15, 81675 München
	Contact(s)	Sahil Gambhir < <a href="mailto:sahil.gambhir@wirelane.com">sahil.gambhir@wirelane.com</a> >
	Entity Type	Charge point manufacturer
Entity 3	Entity Name	Stromnetze Hamburg (SNH)
	Role	DSO
	Address	Stromnetz Hamburg GmbH, Bramfelder Chaussee 130, 22177 Hamburg
	Contact(s)	Dr.-Ing. Annika Magdowski < <a href="mailto:annika.magdowski@stromnetz-hamburg.de">annika.magdowski@stromnetz-hamburg.de</a> >
	Entity Type	DSO
Entity 4	Entity Name	Fraunhofer - Institut für Energiewirtschaft und Energiesystemtechnik IEE
	Role	Provider for DSO Services
	Address	Fraunhofer IEE Königstor 59 34119 Kassel
	Contact(s)	Dr. Sebastian Wende - von Berg
	Entity Type	Pilot Energy Services
Structure of responsibility		Wirelane realizes the contract to the hotels. Stromnetze Hamburg is responsible for the smart grid features and grid environment. Fraunhofer IEE is responsible to provide the Services. KEO is responsible for the EMS and the overall organization of the pilot.
2.3	Rules and procedure	
Meetings		Meetings starts in autumn 2020 every 3 weeks. Pilot Hamburg Meeting with all stakeholders every 2 weeks till 2021 organized by KEO.
Nomination		N/A
Publication of minutes		N/A
2.4	Continual improvement and periodic update	
Meetings		See 3.3

Evaluation procedure	During pilot meeting the evaluation is possible and after the third meeting evaluation will also been done.
----------------------	---

<b>3 DATA MANAGEMENT PLAN</b>		
InterConnect data management plan is the first input.		
<b>3.1 Pilot needs and resources for security and privacy data management</b>		
Ownership of data		Stromnetze Hamburg (SNH) / Hotels
PII Controller		SNH
PII Processors		Fraunhofer IEE
PII Principals		Pilot-Hotels
<b>3.2 Data Management Process</b>		
<b>3.2.1 Agreements</b>		
Agreement approach		<i>To be specified.</i>
Agreement 1	Organizations	<i>To be specified.</i>
	Agreement template	<i>To be specified.</i>
<b>3.2.2 Data description</b>		
Data	Dates for collection	From Q4 2021 to Q3 2023.
	Identification of data	1. Electricity demand of each of five Hotels. 2. Charge point operating and EV data.
	Type of data	1. Critical to service data. 2. Critical to service data.
	Life Cycle	No storage time/deletion process is therefore fixed at this point.
	Data description	To be defined.
<b>3.2.3 Data exchange</b>		
Data flow		1. BeeDIP (Fraunhofer IEE) to EMS via SNH 2. EMS – EVSE – EV 3. CPO - Hotel Guest
Data access control chart		<i>To be specified.</i>
<b>3.2.4 Data access monitoring</b>		
Data access verification procedure		<i>To be specified.</i>
<b>3.2.5 Data Registry</b>		
Registry of agreements		<i>To be specified.</i>
Registry of data sets		<i>To be specified.</i>
Registry of citizen consents		<i>To be specified.</i>

## 4 RISK MANAGEMENT PLAN

The plan will be specified until the m4 meeting.



5	Engineering Management Plan	
	Pilot needs and resources for security and privacy engineering	To be defined within SPOCS meeting.
	Engineering process	Project management driven within Pilot meetings.
	Schedule	Every two weeks.

## 6 CITIZEN ENGAGEMENT PLAN

The pilot does not involve citizens. Not relevant for the project.