



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

WP2 – Domain Interoperable IoT Reference Architecture

**T2.3 - Practice for security and privacy policies
compliance**

**D2.2 - Privacy and Security Design
Principles and Implementation
Guidelines**



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

DOCUMENT INFORMATION

DOCUMENT	D2.2 - Privacy and Security Design Principles and Implementation Guidelines
TYPE	R/DEC/OTHER
DISTRIBUTION LEVEL	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Confidential <input type="checkbox"/> Restricted
DUE DELIVERY DATE	31/12/2020
DATE OF DELIVERY	21/12/2020
VERSION	V1.0
DELIVERABLE RESPONSIBLE	Trialog
AUTHOR (S)	Pierre Mauvy, Antonio Kung, Amélie Gyrard, Yannick Huc (Trialog) Milenko Tasic (VLF)
OFFICIAL REVIEWER/s	Joost Laarakkers, Gerben Broenink (TNO) Fábio André Coelho (INESC TEC)

DOCUMENT HISTORY

VERSION	AUTHORS	DATE	CONTENT AND CHANGES
0.1	Pierre Mauvy Amélie Gyrard Yannick Huc	03/04/2020	Document creation and first version of the ToC and its initial content (STRIDE, LINDDUN, NIST, ISO, etc.)
0.2	Pierre Mauvy	19/06/2020	Integration of partner's feedbacks
0.3	Antonio Kung	24/09/2020	Contribution on vision, state of the art and standards
0.4	Antonio Kung	11/10/2020	Overall contribution
0.5	Amélie Gyrard	12/10/2020	Introduction section Section Microsoft Data Protection/Privacy Mapping Project Section conclusion Annex I Cybersecurity and privacy expertise questionnaire template Annex V Questionnaire Template answered by the pilots
0.6	Antonio Kung	02/11/2020	Correction of templates to be used in Annex
0.7	Milenko Tasic Yannick Huc	16/11/2020	European IoT Platform Initiative projects analysis in context of the InterConnect project Inclusion of first feedback from WP2 partners
1.0	Antonio Kung Yannick Huc	21/12/2020	Inclusion of feedback after review Inclusion of missing content Rewriting of executive summary Final version submitted to the European Commission

INTERNAL REVIEW HISTORY

REVIEWED BY	DATE	SUMMARY OF COMMENTS
Joost Laarakkers (TNO)	14/12/2020	Several smaller comments (as non security expert), put referred tables in chapter 3
Fábio André Coelho (INESC TEC)	16/12/2020	Several smaller comments and editorial modifications
Gerben Broenink (TNO)	16/12/2020	Several smaller comments

EXECUTIVE SUMMARY

This deliverable provides an analysis for security and privacy principles to be applied in Interconnect ICT ecosystems:

- It first provides an overview on H2020 projects that are of interest (AUTOMAT, Create-IoT and IoT platform initiative projects).
- It then describes a number of methodologies that can be useful for ICT ecosystems (STRIDE, LINDDUN, Hoepman design strategies and OASIS-PRMR), provides a survey of standards of interest at the level of ISO/IEC (27001, 27002, 27005, 27110, 27400, 27402, 27403, 27550, 37556, 27561, 27570, 27701, 29134), at the level of ISO (31700) and at the level of IEC (62443), as well as a survey of other references such as NIST material (smart grid cybersecurity, cybersecurity framework, privacy framework, and privacy engineering and risk management), PRIPARE deliverable and Microsoft mapping project.
- It describes two principles, i.e., carry out policy framework analysis and create a security and privacy plan, providing a rationale for these two principles.
- It provides implementation guidelines leading to the creation of a SPP (security and privacy plan).
- It describes the content of a SPP

The deliverable is complemented with six annexes:

- A questionnaire for the pilots,
- A policy framework analysis template,
- A security and privacy plan template,
- Material for security and privacy risk analysis support,
- Results from questionnaires for the pilots, and
- Slides from an internal webinar presenting the concept of security and privacy plan to the pilots.

While the deliverable has included specific considerations on Interconnect domain specific aspects (the domain of Interconnect being smart grid, intelligent buildings and smart home), most of its content is domain independent and could be proposed to other large scale pilots.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
LIST OF FIGURES	8
LIST OF TABLES	9
ABBREVIATIONS AND ACRONYMS	11
1. INTRODUCTION	12
1.1 INTERCONNECT SUMMARY (FROM DOA)	12
1.2 INTERCONNECT CONTRIBUTION ON SECURITY AND PRIVACY (FROM DOA)	12
1.3 INTERCONNECT TASK 2.3 - PRACTICE FOR SECURITY AND PRIVACY POLICIES COMPLIANCE (FROM DOA)	13
1.4 CONTENT OF THIS DELIVERABLE	13
2. COLLECTING WORK ON SECURITY AND PRIVACY	15
2.1 WORK FROM INTERCONNECT RELATED PROJECTS	15
2.1.1 H2020 AUTOMAT D2.5 CYBER SECURITY FRAMEWORK	15
2.1.2 H2020 CREATE-IOT D5.2 IOT POLICY FRAMEWORK DELIVERABLE	17
2.1.3 EUROPEAN IOT PLATFORMS INITIATIVE PROJECTS	20
2.2 SELECTED METHODOLOGIES	27
2.2.1 STRIDE SECURITY THREAT ANALYSIS	28
2.2.2 LINDDUN PRIVACY THREAT ANALYSIS	29
2.2.3 HOEPMAN DESIGN STRATEGIES	30
2.2.4 OASIS PRIVACY MANAGEMENT REFERENCE MODEL METHODOLOGY (PMRM)	31
2.3 SELECTION OF STANDARDISATION WORK ON SECURITY AND PRIVACY	34
2.3.1 ISO/IEC 27001 — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS	34
2.3.2 ISO/IEC 27002 — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	34
2.3.3 ISO/IEC 27005 — INFORMATION SECURITY RISK MANAGEMENT	35
2.3.4 ISO/IEC 27110 (EX 27101) — CYBERSECURITY FRAMEWORK DEVELOPMENT GUIDELINES	35
2.3.5 ISO/IEC 27400 (EX-27030) — SECURITY AND PRIVACY GUIDELINES FOR IOT	36
2.3.6 ISO/IEC 27402 — IOT SECURITY AND PRIVACY – DEVICE BASELINE REQUIREMENTS	36
2.3.7 ISO/IEC 27403 — IOT SECURITY AND PRIVACY – GUIDELINES FOR IOT-DOMOTICS	37
2.3.8 ISO/IEC 27550 — PRIVACY ENGINEERING FOR SYSTEM LIFE CYCLE PROCESSES	37

2.3.9	ISO/IEC 27556 — USER-CENTRIC FRAMEWORK FOR THE HANDLING OF PII BASED ON PRIVACY PREFERENCES	37
2.3.10	ISO/IEC 27561 — PRIVACY OPERATIONALISATION MODEL AND METHOD FOR ENGINEERING (POMME)	38
2.3.11	ISO/IEC 27570 — PRIVACY GUIDELINES FOR SMART CITIES	38
2.3.12	ISO/IEC 27701 — EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS AND GUIDELINES	39
2.3.13	ISO/IEC 29134 — GUIDELINES FOR PRIVACY IMPACT ASSESSMENT	39
2.3.14	ISO 31700 — PRIVACY BY DESIGN FOR CONSUMER GOODS AND SERVICES	40
2.3.15	IEC 62443 SERIES	40
2.4	OTHER REFERENCE DOCUMENTS	41
2.4.1	NIST 7628 – GUIDELINES FOR SMART GRID CYBER-SECURITY	41
2.4.2	NIST CYBERSECURITY FRAMEWORK	41
2.4.3	NIST PRIVACY FRAMEWORK	41
2.4.4	NISTIR 8062 - AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS (FINAL AND DRAFT)	42
2.4.5	PRIPARE PRIVACY AND SECURITY BY DESIGN METHODOLOGY HANDBOOK	42
2.4.6	MICROSOFT DATA PROTECTION/PRIVACY MAPPING PROJECT	42
3.	SECURITY AND PRIVACY PRINCIPLES	44
3.1	RATIONALE FOR THE PRINCIPLES	44
3.1.1	VALUE OF CURRENT WORK ON SECURITY AND PRIVACY	44
3.1.2	CONTRIBUTING TO SECURITY AND PRIVACY FOR ICT ECOSYSTEMS	44
3.1.3	RESULTING PRACTICES FOR ICT ECOSYSTEMS	45
3.2	PRINCIPLE 1: POLICY FRAMEWORK ANALYSIS	45
3.3	PRINCIPLE 2: SECURITY AND PRIVACY PLAN	46
4.	IMPLEMENTATIONS GUIDELINES	47
4.1	SPOCS (SECURITY AND PRIVACY POLICIES COMPLIANCE SOLUTION)	47
4.1.1	DEFINITION OF A SPOCS	47
4.1.2	INTEGRATING THE CONSORTIUM AND THE PILOTS NEEDS IN THE CREATION OF A SECURITY AND PRIVACY PLAN	48
4.1.3	PROCESS TO CREATE A SECURITY AND PRIVACY PLAN	48
4.2	CONTENT OF THE SECURITY AND PRIVACY PLAN	48
4.2.1	GOVERNANCE MANAGEMENT PLAN	49

4.2.2	DATA MANAGEMENT PLAN	49
4.2.3	RISK MANAGEMENT PLAN	50
4.2.4	ENGINEERING MANAGEMENT PLAN	51
4.2.5	CITIZEN MANAGEMENT PLAN	51
5.	CONCLUSION	52
ANNEX I. QUESTIONNAIRE TEMPLATE SENT TO PILOTS: CYBERSECURITY AND PRIVACY EXPERTISE QUESTIONNAIRE		53
ANNEX II. POLICY FRAMEWORK TEMPLATES		55
ANNEX III. SECURITY AND PRIVACY PLAN TEMPLATE		56
ANNEX IV. SECURITY AND PRIVACY RISK ANALYSIS SUPPORT		61
ANNEX V. QUESTIONNAIRE TEMPLATES ANSWERED BY THE PILOTS		68
ANNEX VI. SLIDES OF WEBINAR ON THE CONCEPT OF SECURITY AND PRIVACY PLAN – NOVEMBER 3 RD 2020		75

LIST OF FIGURES

FIGURE 1 AUTOMAT H2020 SYSTEM OF INTEREST	15
FIGURE 2 TARGET GROUP FOR THE IOT POLICY FRAMEWORK.	18
FIGURE 3 MAIN ARCHITECTURE OF SYMBIOTE PROJECT	22
FIGURE 4 RULES FROM BIG IOT PROJECT	23
FIGURE 5 MAIN ARCHITECTURE OF INTER-IOT PROJECT	24
FIGURE 6 MAIN PRINCIPLES OF VICINITY PROJECT	25
FIGURE 7 MAIN ARCHITECTURE OF AGILE IOT PROJECT	26
FIGURE 8 MAIN ARCHITECTURE OF BIOTOPE PROJECT	27
FIGURE 9 THE LINDDUN METHODOLOGY STEPS	29
FIGURE 10. EXAMPLE OF VISUAL MAPPING OF THE MICROSOFT DATA PROTECTION/PRIVACY MAPPING TOOL	43
FIGURE 11. EXAMPLE OF ASSOCIATED MICROSOFT DATA PROTECTION/PRIVACY MAPPING DATASET	43
FIGURE 12 RISK MAP	63

LIST OF TABLES

TABLE 1 – AUTOMAT H2020 CYBERSECURITY FRAMEWORK DELIVERABLE SUMMARY	15
TABLE 2 – AUTOMAT H2020 SECURITY AND PRIVACY RISK ANALYSIS TEMPLATE	17
TABLE 3 – CREATE-IOT H2020 IOT POLICY FRAMEWORK	17
TABLE 4 – CREATE-IOT H2020 TRUST ANALYSIS TEMPLATE	19
TABLE 5 – CREATE-IOT H2020 ENGAGEMENT ANALYSIS TEMPLATE	19
TABLE 6 – CREATE-IOT H2020 SECURITY AND PRIVACY ENGINEERING ANALYSIS TEMPLATE	19
TABLE 7 – IOT EPI PROJECTS	21
TABLE 8 – STRIDE SECURITY THREAT MODEL ADAPTED TO IOT SYSTEMS.....	28
TABLE 9 – LINDDUN PRIVACY THREAT MODEL ADAPTED TO IOT SYSTEMS.....	29
TABLE 10 – EXAMPLE OF MITIGATION ACTIONS PROPOSED IN LINDDUN	30
TABLE 11 – PRIVACY ENGINEERING DESIGN STRATEGIES	30
TABLE 12 – OASIS-PMRM OR POMME STEPS IN ONE ITERATION	31
TABLE 13 – ISO/IEC 29100 PRIVACY FRAMEWORK PRINCIPLES	32
TABLE 14 – OASIS-PMRM PRIVACY CAPABILITIES TAXONOMY	33
TABLE 15 – ISO/IEC 27001 ISMS REQUIREMENTS	34
TABLE 16 – ISO/IEC 27002 INFORMATION SECURITY CONTROLS.....	34
TABLE 17 – ISO/IEC 27005 INFORMATION SECURITY RISK MANAGEMENT	35
TABLE 18 – ISO/IEC 27101 CYBERSECURITY FRAMEWORK DEVELOPMENT GUIDELINES	35
TABLE 19 – ISO/IEC 27400 SECURITY AND PRIVACY GUIDELINES FOR IOT	36
TABLE 20 – ISO/IEC 27402 – IOT SECURITY AND PRIVACY – DEVICE BASELINE REQUIREMENTS.....	36
TABLE 21 – ISO/IEC 27403 IOT SECURITY AND PRIVACY – GUIDELINES FOR IOT DOMOTICS.....	37
TABLE 22 – ISO/IEC 27550 - PRIVACY ENGINEERING FOR SYSTEM LIFE CYCLE PROCESSES	37
TABLE 23 – ISO/IEC 27556 USER-CENTRIC FRAMEWORK FOR THE HANDLING OF PII BASED ON PRIVACY PREFERENCES.....	37
TABLE 24 – ISO/IEC 27561 — PRIVACY OPERATIONALISATION MODEL AND METHOD FOR ENGINEERING (POMME).....	38
TABLE 25 – ISO/IEC 27570 PRIVACY GUIDELINES FOR SMART CITIES	38
TABLE 26 – ISO/IEC 27701 EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS AND GUIDELINES.....	39

TABLE 27 – ISO/IEC 29134 GUIDELINES FOR PRIVACY IMPACT ASSESSMENT	39
TABLE 28 – ISO/IEC 31700 PRIVACY-BY-DESIGN FOR CONSUMER GOODS AND SERVICES	40
TABLE 29 – STRIDE SECURITY THREATS	61
TABLE 30 – LINDDUN PRIVACY THREATS	61
TABLE 31 - IMPACT EXAMPLES	63
TABLE 32 – 27002 CONTROL CATEGORIES	64
TABLE 33 – DATA CONTROLLER PRIVACY CONTROLS	64
TABLE 34 – DATA PROCESSOR PRIVACY CONTROLS	65
TABLE 35 – PIMS-SPECIFIC CONTROL OBJECTIVES AND CONTROLS	65

ABBREVIATIONS AND ACRONYMS

AIOTI	Alliance for Internet of Things Innovation
CNIL	Commission Nationale de l'Informatique et des Libertés
DEI	Digitizing Europe Industry
DOA	Description Of the Action
DFD	Data Flow Diagram
DSF	Demand Side Flexibility
DSO	Distribution System Operator
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
FA	Focus action
GDPR	General Data Protection Regulation
HLA	High Level Architecture
ICT	Information and Communication Technologies
IDS/IDP	Intrusive Detection System/Intrusive Preventive System
IEC	Internal Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
LSP	Large Scale Pilot
NIST	National Institute of Standard and Technology
NISTIR	NIST Interagency/Internal Report
OEM	Original Equipment Manufacturer
P2P	Peer to Peer
PII	Personal Identifiable Information
QoS	Quality of Service
SASL	Simple Authentication and Security Layer
SPOCS	Security and Privacy Policy Compliance Solution
SPP	Security and Privacy Plan
W3C	World Wide Web Consortium
XMPP	eXtensible Messaging and Presence Protocol

1. INTRODUCTION

1.1 INTERCONNECT SUMMARY (FROM DOA)

InterConnect envisages to contribute for the democratization of efficient energy management, through a flexible and interoperable ecosystem where demand side flexibility can be soundly integrated with effective benefits to end-users.

In fact, over the last few years several projects and technology providers have come up with solutions that allow every energy user to have awareness and control over his appliances, but there has always been a major issue with interoperability. End-users should be able to choose and change their technology providers, without having to replace their installation, every time they feel this need and still be able to adopt sustainable behaviour and benefit from technological advances.

In the energy sector, a steep move towards digital is occurring and becoming tremendously user-centric and market-driven. The system dimension is significant, as the number of energy service providers is increasing thanks to favourable regulatory environment and technology advancements for monitoring and control.

This is the reason why this consortium integrates relevant partners from all the representative stakeholders in this new energy paradigm. Specific competences in ICT, IoT, energy, data science, software, were included and the full value chain, from R&D institutions, manufacturers, DSO, retailers, IT providers, and energy users is represented.

To guarantee a higher Europe-wide impact, several relevant associations related with ICT and energy are also involved. To achieve a significant dimension, 7 large scale pilots, in different countries and with different type of end-users, are foreseen to guarantee representativeness and dimension in terms of number of appliances and services. The overarching objective of these pilots is to demonstrate a real digital market environment over electrical systems with significant amounts of DSF, reducing operational and investment costs that will benefit energy end-users and help EU achieve its energy efficiency objectives.

1.2 INTERCONNECT CONTRIBUTION ON SECURITY AND PRIVACY (FROM DOA)

Interconnect focuses on building policy and regulatory compliance on security and privacy. It will follow the following approach for multi-domain security and privacy in WP5:

- defining and practicing security and privacy management from a lifecycle and ecosystem viewpoint integrating cybersecurity frameworks and privacy-by-design;
- addressing the issue of secure and privacy interoperation from policy management perspective leveraging recent advances in trust management, trust delegation, using role-based access control, and privacy preference management;

- creating a consensus on the approach through the BRIDGE initiative, collaboration with the OpenDei¹ CSA focusing on the digital transformation of European industry, and through the establishment of a standardisation plan, taking into account current work, such as ISO/IEC 27400² or ISO/IEC 30149³ (“IoT - trustworthiness framework”). This will lead to the proposal of new standards (in WP9), focusing on multi-lateral security and privacy for smart homes and grids.

1.3 INTERCONNECT TASK 2.3 - PRACTICE FOR SECURITY AND PRIVACY POLICIES COMPLIANCE (FROM DOA)

The objective of task 2.3 is to define a coordinated security and privacy practice for future IoT ecosystems, for the integration of smart homes/buildings with smart grids. A global pro-active framework will be defined, including

- a security and privacy-by-design practice (based on AIOTI reference architecture, ISO IoT reference architecture covering the cybersecurity lifecycle such as ISO/IEC 27101⁴, NIST guidelines for smart grid cyber-security-NISTIR 7628- and current privacy-by-design standards); and
- redefinition of governance role and the compliance auditing role.

This deliverable focusses on policy compliance. The T2.3 architecture guidelines and requirements for the InterConnect architecture are part of D2.1.

1.4 CONTENT OF THIS DELIVERABLE

The objectives of the deliverable are the following:

- Identify security and design principles which:
 - will guide the work of the pilots to ensure their security and privacy compliance,
 - will be assessed towards the end of the project for adoption in future industrial IoT deployment on energy.
- Provide implementation guidelines to pilots:
 - a solution called SPOCS (Security and Privacy Policy Compliance Solution) is defined
 - the solution includes (1) a security and privacy plan template, and (2) a process based on workshops to develop a security and privacy plan based on a template

The deliverable is structured as follows:

¹ <https://www.opendei.eu/>

² IoT security and privacy – guidelines (formerly ISO/IEC 27030), at committee draft stage

³ IoT trustworthiness principles (formerly IoT trustworthiness framework), at working draft stage

⁴ Guidelines for cybersecurity framework, inspired from the NIST cybersecurity framework, at publication stage

- a survey of existing work is provided
 - contributions on security and privacy from various collaborative projects
 - contributions on methodologies
 - contributions on security and privacy in standardisation
 - other contributions
- a resulting set of security and privacy principles is proposed
- implementation guidelines are provided
 - the SPOCS process is described
 - the template is provided
 - the workshop approach is explained

2. COLLECTING WORK ON SECURITY AND PRIVACY

The objective of this section is to derive security and privacy principles, i.e. high-level requirements and approaches that can be used in InterConnect.

2.1 WORK FROM INTERCONNECT RELATED PROJECTS

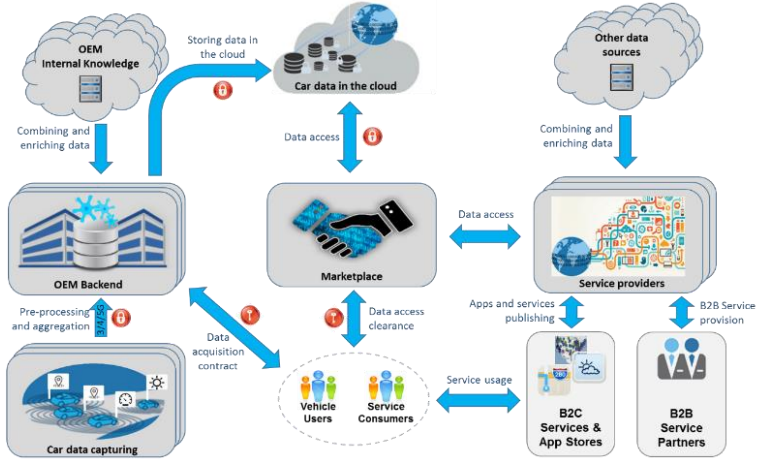
Many collaborative projects (past projects or on-going projects) have applied security and privacy practices. This section focuses on a selection of projects involving InterConnect partners as well as European IoT Platform Initiative projects:

- The same template description for each project is used to ease analysis,
- The content of the description focuses on reusable security and privacy building blocks.

2.1.1 H2020 AUTOMAT D2.5 CYBER SECURITY FRAMEWORK

Trialog was the editor of this deliverable.

TABLE 1 – AUTOMAT H2020 CYBERSECURITY FRAMEWORK DELIVERABLE SUMMARY

<p>Brief description of project</p>	<p>AUTOMAT is one of the first H2020 big data projects. It involves an ecosystem. As stated in the project description:</p> <p><i>The core intention of the AutoMat project is to innovate an open ecosystem for Vehicle Big Data, materializing in the form of a cross-border Vehicle Big Data Marketplace that leverages currently unused information gathered from the large amount of vehicles of various brands. The interface to the market-place is derived from a Common Vehicle Information Model that makes mined and anonymous vehicle data from various OEMs accessible to cross-sectorial service providers. With the huge amount of volatile data from vehicles, the AutoMat ecosystem heavily builds upon current trends in Big Data. Exemplary service scenarios, driven by service providers dedicated to generate concrete businesses from the AutoMat ecosystem, are developed in the context of meteorological data based hyper local and extended innovative enterprise service domains.</i></p>
<p>System of interest</p>	 <p>FIGURE 1 AUTOMAT H2020 SYSTEM OF INTEREST</p>

	<p>Figure 1 shows AUTOMAT system of interest, an ecosystem consisting of the following components:</p> <ul style="list-style-type: none"> • The Proprietary Vehicle Data Sources (car data capturing) • The OEM (automotive manufacturer) Backend • The Cloud storage provider (car data in the cloud) • The Vehicle Big Data Marketplace • The Service Provider
Deliverable	Published in March 2018, available at the following URL: https://automat-project.eu/sites/default/files/automat/public/content-files/articles/Automat-D2.5_Cyber%20security%20framework.pdf
Relationship to InterConnect	Data exchange and data space system will be a key capability of an IoT energy ecosystem
Security and privacy principles	<ul style="list-style-type: none"> • Considerations on ethical and legal aspects • Guidance for a security and privacy-by-design process, based on existing work (PRIPARE⁵ and its ISO sequel – ISO/IEC 27550 – Privacy Engineering⁶) • A common security and privacy risk analysis, applied to each component of the ecosystem: <ul style="list-style-type: none"> ○ Characterisation of the component (actors, use cases, typical architecture entities) ○ Typical Business and contractual cybersecurity capabilities ○ Typical privacy and security threats ○ Typical breaches and impact ○ Typical measures to lower the likelihood of threats • Each component analysis was based on guidance provided by ISO/IEC 29134 (Privacy Impact Assessment⁷).
Impact of this project	<p>AUTOMAT has contributed to ISO/IEC 20547-4 (Big data security and privacy), which includes</p> <ul style="list-style-type: none"> • a section on ecosystem requirements that are the result of AUTOMAT work • an annex describing the AUTOMAT ecosystem
What can be reused in InterConnect	The following template can be reused. The AUTOMAT deliverable provides examples on resulting security and privacy analysis

⁵ <http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf>

⁶ Underway. Trialog is the editor of ISO/IEC 27550

⁷ Published in June 2017 (<https://www.iso.org/standard/62289.html>)

TABLE 2 – AUTOMAT H2020 SECURITY AND PRIVACY RISK ANALYSIS TEMPLATE		
	Security and privacy analysis template	
	Characterisation of the component (actors, use cases, typical architecture entities)	To be provided by pilot
	Typical Business and contractual cybersecurity capabilities	To be provided by pilot
	Typical privacy and security threats	To be provided by pilot
	Typical breaches and impact	To be provided by pilot
	Typical measures to lower the likelihood of threats	To be provided by pilot
Conclusion	Interconnect will carry out for each pilot a security and privacy risk analysis. It will use the security and privacy risk analysis template in annex IV which takes into account the result of AUTOMAT, the previous practice of past IoT large scale pilots, and the advance provided by standardisations.	

2.1.2 H2020 CREATE-IOT D5.2 IOT POLICY FRAMEWORK DELIVERABLE

Trialog was the editor of this deliverable.

TABLE 3 – CREATE-IOT H2020 IOT POLICY FRAMEWORK

Brief description of project	<p>CREATE-IoT is the predecessor of OpenDei. As stated in the project website⁸: <i>CREATE-IoT’s aim is to stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. This requires synchronisation and alignment on strategic and operational terms through frequent, multi-directional exchanges between the various activities under the IoT Focus Areas (FAs). It also requires cross fertilisation of the various IoT Large Scale Pilots (LSPs) for technological and validation issues of common interest across the various application domains and use cases.</i></p> <p><i>CREATE-IoT aligns the activities with the Alliance for Internet of Things Innovation (AIOTI) and will coordinate and support the upcoming LSPs in sustaining the ecosystems developed during those projects through mapping the pilot architecture approaches, address interoperability and standards approaches at technical and semantic levels for object connectivity, protocols, data formats, privacy, security, trusted IoT, open APIs and share the road-mapping with international initiatives.</i></p>
System of interest	<p>The system of interest is any IoT large scale pilot. As showed in the deliverable</p>

⁸ <https://european-iot-pilots.eu/create-iot/>

	<div> <div> <div>Return from experience</div> <div> <div>LSP IoT Policy framework Create-IoT D5.1 – D5.2</div> <div> <div>supports</div> <div>Contributes</div> </div> <div> <div>Large Scale Pilots</div> <div>Future IoT deployments</div> </div> </div> </div> </div> <p>FIGURE 2 TARGET GROUP FOR THE IOT POLICY FRAMEWORK.</p> <p>Figure 2 shows the objective of the IoT policy framework deliverable:</p> <ul style="list-style-type: none"> • A first version was made available to the large-scale pilots (D5.1⁹) stakeholders • Further to the large-scale pilot operation, D5.2 was published, summarizing the large-scale pilots experience, but also providing input to an IoT policy framework that will be used for deployment.
Deliverable	Published in January 2020, available at the following URL: https://european-iot-pilots.eu/wp-content/uploads/2020/06/D05_02_WP05_H2020_CREATE-IoT_Final.pdf
Relationship to InterConnect	Create-IoT was the support action associated with the Monica, Synchronicity, Activage, Autopilot IoT large scale pilots. Its results are input to OpenDei and the current IoT large scale pilots
Security and privacy principles	<ul style="list-style-type: none"> • The work took into account current work at standardisation level from ITU-T, ISO/IEC JTC1 (WG13, AG8, SC27, SC38, SC41, SC42), ISO PC317, ISO TMBG, ISO CASCO, ISO TC22/SC32/WG11) • Create-IoT took a policy viewpoint that Trust is a key concern to be addressed in an IoT policy framework. Policies include a socio-economic, a business and a technical dimension. Policies must take into account the following: <ul style="list-style-type: none"> ○ IoT bridges the virtual/digital world with the physical world ○ IoT covers complex interactions in an ecosystem ○ IoT is based on complex architecture considerations that have to integrate technical properties such as security, safety, reliability, connectivity, resilience, availability, dependability, privacy. • Organisation engagement is a key prerequisite for successful IoT. An IoT policy framework should include: <ul style="list-style-type: none"> ○ Measures for ethics engagement, e.g. applying a systematic ethics impact assessment.

⁹ https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf

18 | 75

	<ul style="list-style-type: none"> ○ Measures for standardisation engagement. ○ Measures for legislation engagement. ○ Measures for contracts engagement. • Security and privacy are key cross-cutting capabilities to engineer for IoT. An IoT policy framework should include: <ul style="list-style-type: none"> ○ Policies on citizen engagement and user-centred processes. ○ Policies on the development of supporting tools ○ Policies on the integration of security, privacy and other properties ○ Policies on data protection by design integrating the lifecycle ○ Policies on the definition of organisation roles in an IoT ecosystem ○ Policies for building and using common engineering knowledge ○ Policies for common security and privacy engineering methods 																										
Impact of this project	<p>Common building blocks resulting from the work of five large scale pilots (Activage, Autopilot, IoF2020, Monica, Synchronicity).</p> <p>Influence on a number of new standards under development on security and privacy (e.g. ISO/IEC 27101, 27400, 27402, 27403, 27556, 27570).</p>																										
What can be reused in InterConnect	<p>The following templates can be reused. The deliverable provides examples on resulting analysis provided by the IoT large scale pilots.</p> <p>TABLE 4 – CREATE-IOT H2020 TRUST ANALYSIS TEMPLATE</p> <table border="1"> <tr> <th colspan="2">Trust analysis template</th></tr> <tr> <td>Socio-economical perspective</td><td>To be provided by pilot</td></tr> <tr> <td>Business perspective</td><td>To be provided by pilot</td></tr> <tr> <td>Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)</td><td>To be provided by pilot</td></tr> </table> <p>TABLE 5 – CREATE-IOT H2020 ENGAGEMENT ANALYSIS TEMPLATE</p> <table border="1"> <tr> <th colspan="2">Engagement analysis template</th></tr> <tr> <td>Engagement on ethics</td><td>To be provided by pilot</td></tr> <tr> <td>Engagement on standards</td><td>To be provided by pilot</td></tr> <tr> <td>Engagement on legislation</td><td>To be provided by pilot</td></tr> <tr> <td>Engagement on contracts</td><td>To be provided by pilot</td></tr> </table> <p>TABLE 6 – CREATE-IOT H2020 SECURITY AND PRIVACY ENGINEERING ANALYSIS TEMPLATE</p> <table border="1"> <tr> <th colspan="2">Security and privacy analysis template</th></tr> <tr> <td>Risk management (use the Automat security and privacy risk analysis template, see Table 2)</td><td>To be provided by pilot</td></tr> <tr> <td>Designing security and privacy:</td><td>To be provided by pilot</td></tr> <tr> <td>Assuring security and privacy</td><td>To be provided by pilot</td></tr> </table>	Trust analysis template		Socio-economical perspective	To be provided by pilot	Business perspective	To be provided by pilot	Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	To be provided by pilot	Engagement analysis template		Engagement on ethics	To be provided by pilot	Engagement on standards	To be provided by pilot	Engagement on legislation	To be provided by pilot	Engagement on contracts	To be provided by pilot	Security and privacy analysis template		Risk management (use the Automat security and privacy risk analysis template, see Table 2)	To be provided by pilot	Designing security and privacy:	To be provided by pilot	Assuring security and privacy	To be provided by pilot
Trust analysis template																											
Socio-economical perspective	To be provided by pilot																										
Business perspective	To be provided by pilot																										
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	To be provided by pilot																										
Engagement analysis template																											
Engagement on ethics	To be provided by pilot																										
Engagement on standards	To be provided by pilot																										
Engagement on legislation	To be provided by pilot																										
Engagement on contracts	To be provided by pilot																										
Security and privacy analysis template																											
Risk management (use the Automat security and privacy risk analysis template, see Table 2)	To be provided by pilot																										
Designing security and privacy:	To be provided by pilot																										
Assuring security and privacy	To be provided by pilot																										

Conclusion	We plan to reuse this template (see Annex II) to allow comparison with past IoT large scale pilots
------------	--

2.1.3 EUROPEAN IOT PLATFORMS INITIATIVE PROJECTS

The European IoT Platforms¹⁰ Initiative (IoT EPI) includes 7 projects focusing on different challenges of interoperability within and among IoT platforms and systems. 6 of the initiative’s projects which are of interest for InterConnect are:

- symbloTe¹¹ offers a middleware framework covering all seven layers of the IoT Architecture. Existing IoT platforms and services can use symbloTe's Core Services to register and discover other functions. One of symbloTe's key features is its flexible and incremental approach to interoperability; ranging from purely syntactic and semantic to full ecosystems where smart objects can interact, project stakeholders could choose which interoperability level they wished to support. Security mechanisms are based on resource access schemes and identity management.
- The BIG IoT¹² initiative focuses on the upper layers of the IoT architecture, through its API for resource sharing and discovery. BIG IoT's Marketplace offers additional resources to expand the project's ecosystem, such as billing, subscription, and accounting. Some flexibility was included in the project after identifying different types of IoT platforms and their specific requirements (e.g., always-on, constrained device, etc.). Semantic and syntactic interoperability is achieved via the definition of a core model, extended with domain-independent and domain-specific vocabularies.
- INTER-IoT¹³ focuses on six layers of the IoT Architecture, covering aspects ranging from physical components, network connectivity to QoS, and resource catalogue for service registering and discovery. A practical approach to security was privileged in this project, including multiple control points based on best practices. Interoperability is achieved by translating each IoT platform's resources to INTER-IoT's common ontology model and its extensions.
- VICINITY¹⁴ addresses the five upper layers of the IoT Architecture and builds around the concept of "virtual neighborhoods" to achieve interoperability across distributed (i.e., P2P) IoT ecosystems. VICINITY's semantic and syntactic interoperability approach is based on a single common ontology - defined by the project - and extended through domain-specific ontologies, guided by the project requirements and defined use cases.
- AGILE IoT¹⁵ provides a flexible and modular hardware and software solution for building interoperable IoT solutions. The software modules cover functions such as device

¹⁰ <https://iot-epi.eu/>

¹¹ <https://www.symbiote-h2020.eu/>

¹² <http://big-iot.eu/>

¹³ <https://inter-iot.eu/>

¹⁴ <https://vicinity2020.eu/vicinity/>

¹⁵ <http://agile-iot.eu/>

management, communication networks, and solution for distributed storage. The hardware module focuses on extending the Raspberry Pi platform's capabilities by including additional radio sockets and expanding its connectivity options.

- bloTope¹⁶ follows a system-of-system approach for building an open, interoperable ecosystem, allowing for rapid use case implementation. bloTope's architectural framework is built around a set of scalable micro-services. Interoperability is achieved via the implementation of the Open Messaging Interfaces (O-MI) and the Open Data Format (O-DF), defined by The Open Group.

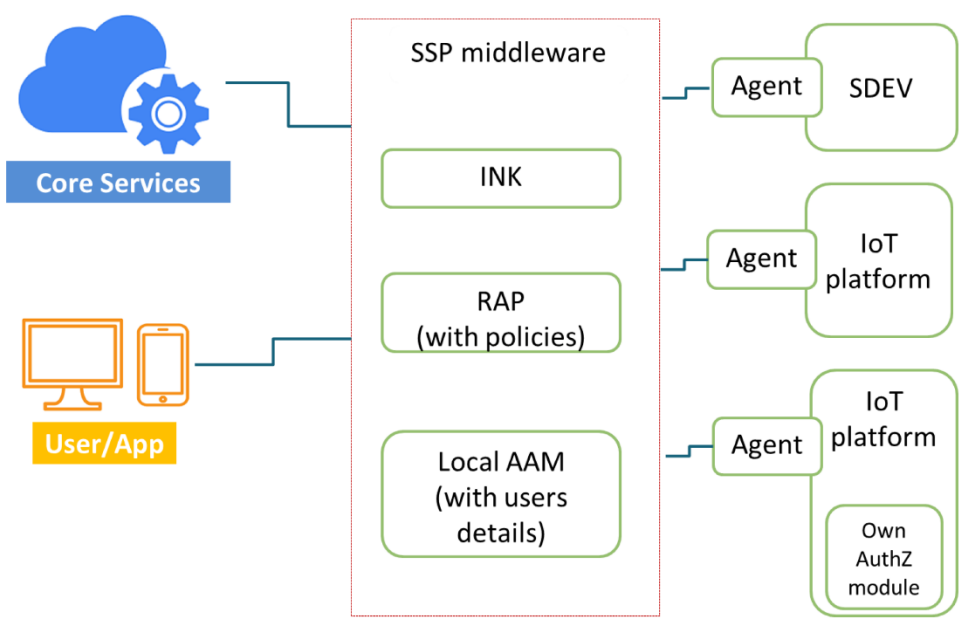
All listed projects have ended and they have produced final reports. Since InterConnect addresses semantic interoperability between smart building and energy systems, it is important to draw conclusions from the IoT EPI projects on the main requirements, challenges and results with respect to interoperability between IoT systems and general interoperability on syntactic and semantic level between services and platforms belonging to different stakeholders and utilizing different base technologies.

More information about IoT EPI projects and their relation with the InterConnect project can be found in InterConnect deliverable D5.1 “Concept, design and architecture of the interoperable marketplace toolbox”. Table below provides a short overview of the main concepts for security and data/privacy protection utilized and demonstrated by the relevant IoT EPI projects.

TABLE 7 – IOT EPI PROJECTS

IoT EPI project	Approach for security and privacy protection, relevant deliverable and impact on InterConnect
symbloTe	<div>Security and data protection principles and solutions:</div> <ul style="list-style-type: none"> symbloTe’s security mechanisms are incorporated into various architectural domains, based on resource access schemes and identity management. To this end, symbloTe implements Attribute-Based Access Control (ABAC) mechanisms, where access rights are granted to users (i.e., client application or resources within a system) possessing the exact set of attributes that match the predefined access policy. Each access policy can be defined as a combination of attributes (i.e., user, resource, environment, etc.), allowing for complex policies based on Boolean logic (IF, THEN) and inclusive/exclusive logic (AND, OR).

¹⁶ <https://biotope-project.eu/>

	<div>  </div> <p>FIGURE 3 MAIN ARCHITECTURE OF SYMBIOTE PROJECT</p> <p>Relevant deliverables:</p> <ul style="list-style-type: none"> • D3.2 – Resource trading, security and federation mechanisms • D4.2, D4.3 – First/Final symbloTe middleware implementation <p>Impact on InterConnect:</p> <ul style="list-style-type: none"> • Implement attribute-based access control mechanisms as part of the interoperability adapters so that service providers can configure custom access control rules. Investigate and reuse best practices from symbloTe approach regarding the attribute-based access control.
BIG IoT	<p>Security and data protection principles and solutions:</p> <ul style="list-style-type: none"> • Security on API level - must be exchangeable to adapt to new risks. • Decentralized, federated or delegated authentication • Large effort on data minimization - privacy protection. • Using privacy icons from Aza Raskin. • Detailed risk identification and severity estimation mechanism. • Identity management - attribute based.

	<div> <p> Your Data May be Used for Purposes You Do Not Intend Your Data is Used Only for the Intended Use Your data may be bartered or sold. Your data is never bartered or sold. </p> <p> Data may be given to law enforcement even when legal process is not followed. Data is given to law enforcement only when legal process is followed. Site gives your data to advertisers. Your data is never given to advertisers. </p> <p> Your data is kept for less than 1 month. 3 months 6 months 18 months Your data may be kept indefinitely. </p> </div> <p>FIGURE 4 RULES FROM BIG IOT PROJECT</p> <p>Relevant deliverables:</p> <ul style="list-style-type: none"> D3.3 – Security and privacy designs for smart objects. <p>Impact on InterConnect:</p> <ul style="list-style-type: none"> InterConnect project will apply similar approach for labelling privacy protection risks and capabilities of services. Other labelling approaches will also be assessed. These labels will be part of the semantic interoperability layer and ontology so that reasoning functionalities can use them.
INTER-IoT	<p>Security and data protection principles and solutions:</p> <ul style="list-style-type: none"> Following the project’s focus on potentially vulnerable sectors (e.g., the health sector handles personally identifiable data), a practical approach to cybersecurity was privileged. This can be translated by INTER-IoT’s cross-layered approach for data confidentiality, integrity, availability, and overall quality of service (QoS). The resulting framework (SecurIoTy) provides a scalable security protocol, covering all architectural components, ranging from secure data traffic from/to devices to encrypted data storage for applications. To achieve this, INTER-IoT provides multiple control points, based on industry best practices and standard protocols (e.g., HTTP(S), WebDAV, REST, TCP).

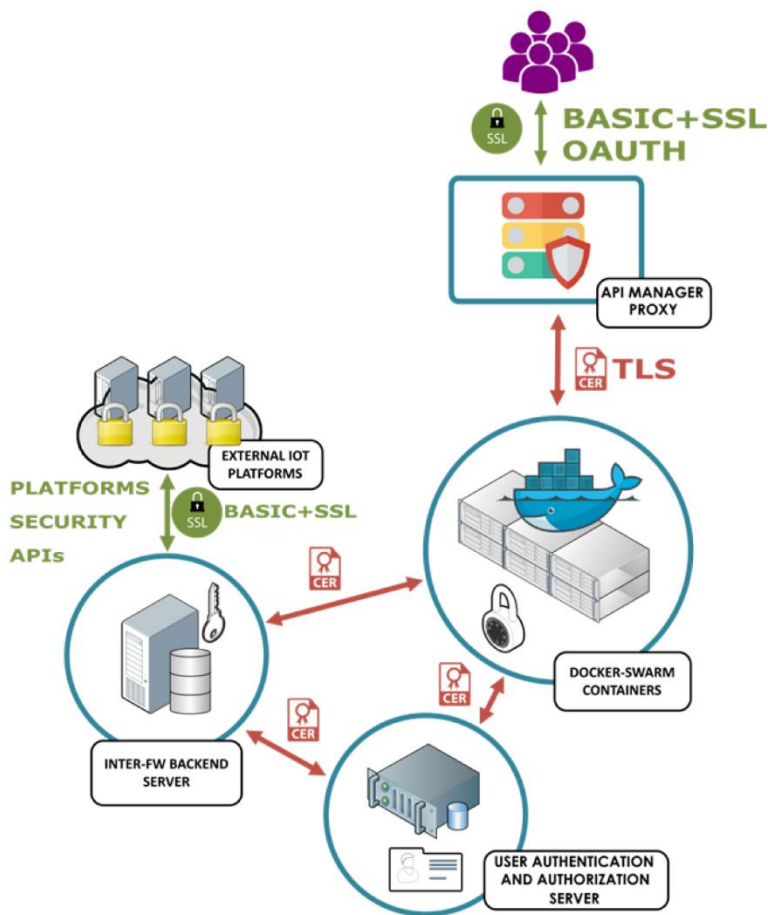


FIGURE 5 MAIN ARCHITECTURE OF INTER-IOT PROJECT

Relevant deliverables:

- D4.2 – Final reference IOT platform meta architecture and meta data model
- D4.3 – Initial reference IOT platform meta architecture meta data model and interoperable IoT framework model and engine v1

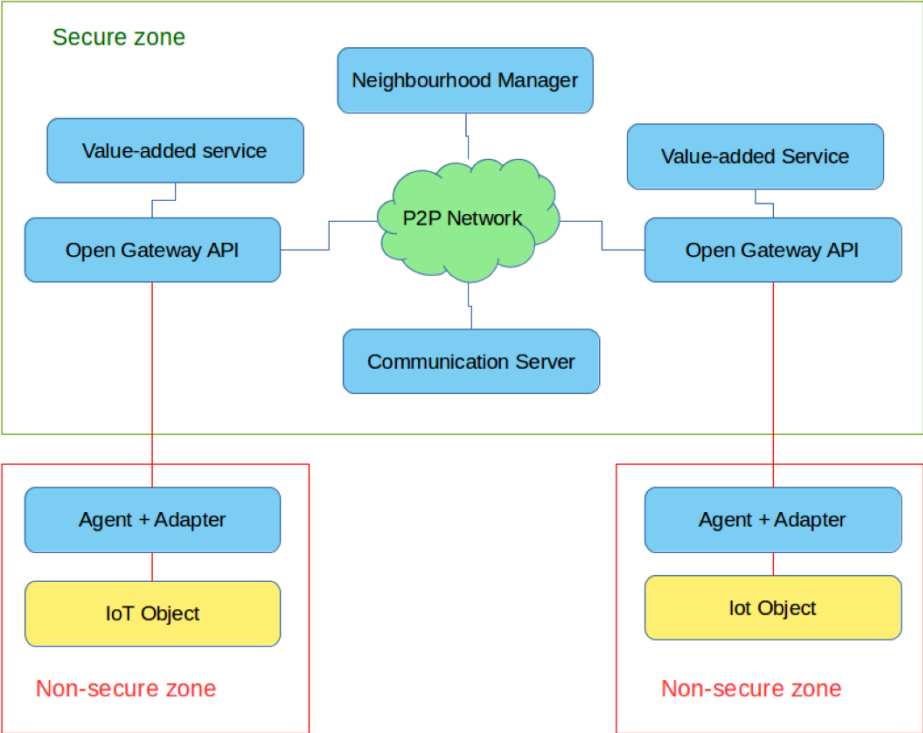
Impact on InterConnect:

- InterConnect project will implement service container manager (e.g. based on Docker or other technologies) with security principles validated in Inter IoT project.

VICINITY

Security and data protection principles and solutions:

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

	<div data-bbox="442 253 1369 983">  </div> <p>FIGURE 6 MAIN PRINCIPLES OF VICINITY PROJECT</p> <p>Relevant deliverables:</p> <ul style="list-style-type: none"> • D4.3 – Vicinity security services <p>Impact on InterConnect:</p> <ul style="list-style-type: none"> • InterConnect project will explore application of secure-zone approach as part of its semantic interoperability framework and investigate if this can be implemented as part of ontology and reasoning. A step towards this is already made in D2.1 with the security groups.
AGILE IoT	<p>Security and data protection principles and solutions:</p> <ul style="list-style-type: none"> • The project follows an attribute-based approach to security. Some of the project’s key security features are: user authentication and registration; entity registration (e.g., for devices such as sensors, OAuth2 clients, etc.); attribute management, allowing for the implementation of various access control mechanisms, such as role-based access control; group management, for defining security policies within a specific group; credential management, which stores credentials for accessing external clouds or systems. • Identity management components provide authentication mechanisms and administer attributes and credentials for the system’s entities. • Attribute based identity model and management. Apart from users, identity manager is used by the core components of the AGILE platform.

	<div data-bbox="517 264 1284 723"> <p>The diagram illustrates the main architecture of the Agile IoT Project. It is divided into two main sections: the Agile Identity Management (IDM) system and the Oauth2 server. The Agile IDM system is enclosed in a dashed box and includes a REST Entity API at the top, which interacts with the Agile-idm-core. The Agile-idm-core contains Schema Validation and Policy Enforcement & Declassification modules. Below this is the Agile-idm-entity-storage, which interacts with the Agile-web-ui at the bottom. A central Token Storage module acts as a hub, connecting to the REST Entity API, the Agile-idm-core, the Agile-idm-entity-storage, and the Oauth2 server. The Oauth2 server section includes an Oauth2 server API at the top, which interacts with an Oauth2-orize module. This module is connected to the Token Storage and an Authentication providers module. The Authentication providers module lists Google, Github, PAM, Agile-Local, and WebId as supported providers.</p> </div> <div data-bbox="533 772 1268 801"> <p>FIGURE 7 MAIN ARCHITECTURE OF AGILE IOT PROJECT</p> </div> <div data-bbox="339 824 655 855"> <p>Relevant deliverables:</p> </div> <div data-bbox="387 882 1193 1003"> <ul style="list-style-type: none"> • D5.1 – First prototype of AGILE identity management • D5.2 – User control and provenance management • D5.3 – Secure data sharing. </div> <div data-bbox="339 1023 683 1057"> <p>Impact on InterConnect:</p> </div> <div data-bbox="387 1081 1466 1276"> <ul style="list-style-type: none"> • InterConnect project will implement authentication mechanism supported with Oauth2 protocol and results and implementation from AGILE IoT will be used as a reference. AGILE IoT role based access control will be considered as one of the policies for the InterConnect attribute based access control. </div>
<div data-bbox="129 1420 244 1451"> bioTope </div>	<div data-bbox="339 1310 1091 1341"> <p>Security and data protection principles and solutions:</p> </div> <div data-bbox="387 1368 1466 1563"> <ul style="list-style-type: none"> • The Security & Privacy block provides the required security mechanisms as a service. Security is provided on two levels: the first covers secure authentication and permission methods (i.e., based on OAuth); the second covers secure data transfer and identity management (i.e., MIST). </div>

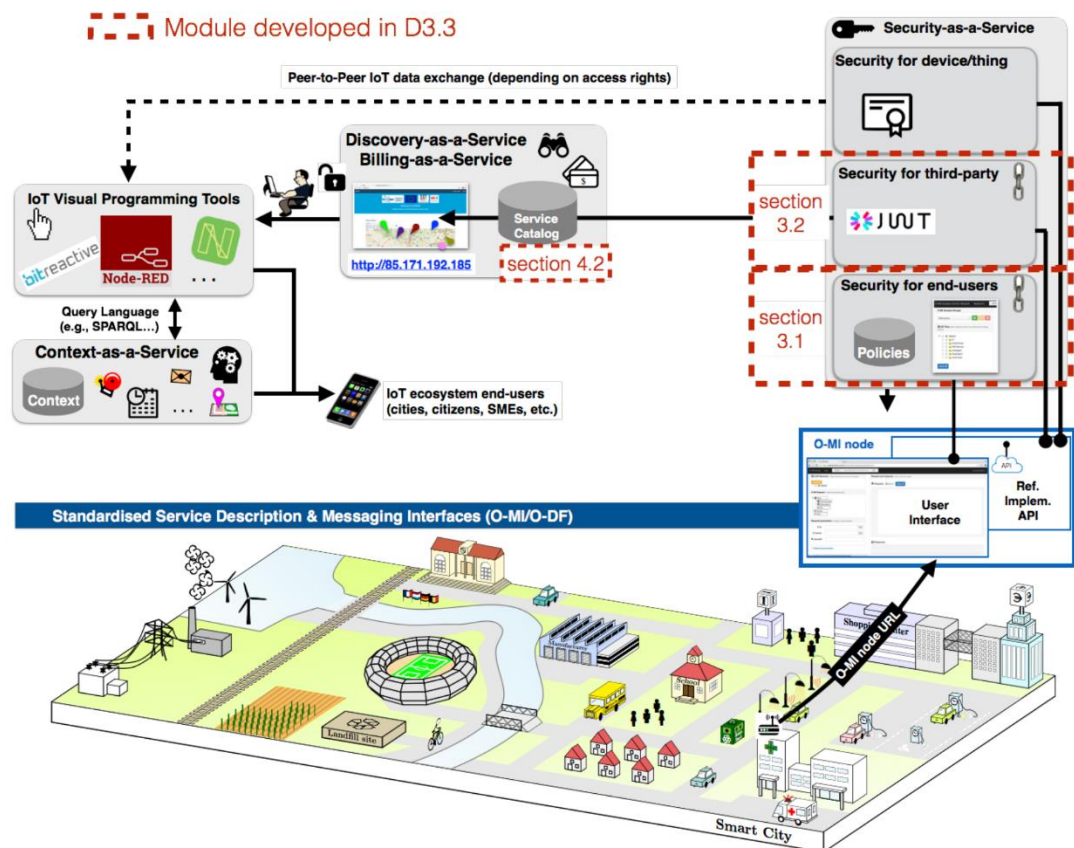


FIGURE 8 MAIN ARCHITECTURE OF BIOTOPE PROJECT

Relevant deliverables:

- D3.1/D3.7 – Framework for identity creation, management and authentication v1/v2
- D3.3 - Context-sensitive security, privacy management, adaptation framework v1

Impact on InterConnect:

- InterConnect project will investigate biotope project approach for security as a service and assess potential for applying the main concepts as one of the policies of the configurable attribute access control mechanisms to be integrated with semantic interoperability adapters.

2.2 SELECTED METHODOLOGIES

The proposed practice to the InterConnect pilots should include a security and privacy threat analysis methodology. The practice from previous projects (Automat, Large scale pilots supported by Create-IoT) were based on the STRIDE and the LINDDUN threat analysis methodologies

2.2.1 STRIDE SECURITY THREAT ANALYSIS

System designers must consider threats when designing their architecture system and ask the following questions: 1) How can an attacker change the authentication data? 2) What is the impact if an attacker can read the user profile data? and 3) What happens if access is denied to the user profile database?

STRIDE¹⁷ threats are grouped in six categories:

- **Spoofing identity** (e.g., illegally accessing and using another user's authentication information, such as username and password).
- **Data Tampering** involves the malicious modification of data (e.g., unauthorized changes made to persistent data within in a database, and the alteration of data in transit over the Internet.
- **Repudiation** is associated with users who deny performing an action without other parties having any way to prove (e.g., a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations). **Non-Repudiation** refers to the ability of a system to counter repudiation threats (e.g., users purchasing items might have to sign for the item upon receipt. The vendor can use the signed receipt as a proof that the user received the package).
- **Information disclosure** involves the exposure of information to individuals who are not supposed to have access to it (e.g., the users read a file that they were not granted access to, or an intruder to read data in transit between two computers).
- **Denial of service** (DoS) attacks deny service to valid users (e.g., a Web server temporarily unavailable). It hinders system availability and reliability.
- **Elevation of privilege**, the users gain privileged access to compromise or destroy the entire system. The attacker has penetrated all system defences and become part of the trusted system itself.

TABLE 8 – STRIDE SECURITY THREAT MODEL ADAPTED TO IOT SYSTEMS

	Threat	Property	Property description
IoT systems security objectives expressed as threats to counter	Spoofing	Authentication	The identity of IoT entities or IoT users is established (or you are willing to accept anonymous entities).
	Tampering	Integrity	IoT data and system resources are only changed in appropriate ways by appropriate people.
	Repudiation	Nonrepudiation	IoT users cannot perform an action and later deny performing it.
	Information disclosure	Confidentiality	Data is only available to the IoT users intended to access it.
	Denial of Service	Availability	IoT services are ready when needed and perform acceptably.
	Elevation of privilege	Authorization	IoT users are explicitly allowed or denied access to resources.

Note that the term IoT systems is according to ISO/IEC 30141 IoT reference architecture. It can refer to a subsystem or a platform.

¹⁷ STRIDE. The STRIDE threat model, 2009. [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN)

2.2.2 LINDDUN PRIVACY THREAT ANALYSIS

LINDDUN¹⁸ is a privacy counterpart of STRIDE that integrates 7 main privacy threat categories: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance.

TABLE 9 – LINDDUN PRIVACY THREAT MODEL ADAPTED TO IOT SYSTEMS

	Threat	Property		Property description
IoT systems privacy objectives expressed as threats to counter	Linkability	Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information associated with IoT entities or IoT users.
	Identifiability		Anonymity	Hiding the link between an IoT user or an IoT entity identity and an action or a piece of information
	Non-repudiation		Plausible deniability	Ability for an IoT end user or and IoT entity to deny having performed an action that other parties can neither confirm nor contradict
	Detectability		Undetectability and unobservability	Hiding the activities of an IoT user or an IoT entity.
	Disclosure of information	Security	Confidentiality	Ability of the IoT system to hide the data content or to control the release of data content
	Unawareness	Soft Privacy	Content awareness	IoT user's consciousness regarding his own data
	Non-compliance		Policy and consent compliance	IoT stakeholder who is a PII controller to inform the IoT user who is a PII principal on the IoT system's privacy policy, or allow the IoT user to specify consents in compliance with legislation

As illustrated in Figure 9, LINDDUN methodology steps are divided in problem space steps (step 1-3), which aim at describing privacy threats, and in solution space steps (step 4-6) necessary for the elicitation of mitigation measures and solutions corresponding to the threats identified.

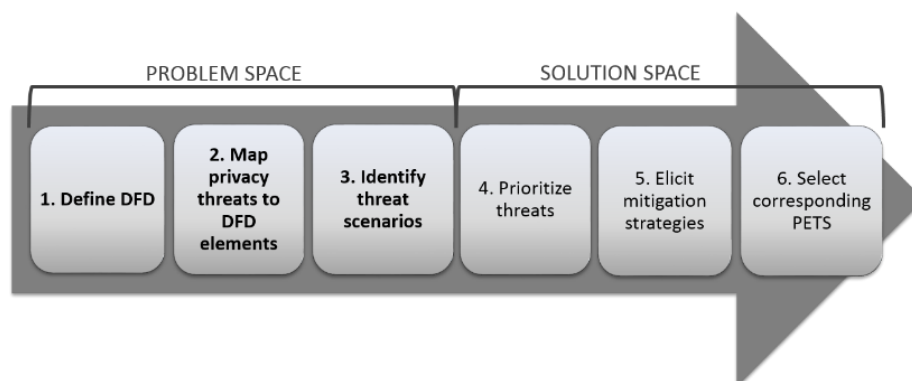


FIGURE 9 THE LINDDUN METHODOLOGY STEPS

¹⁸ LINDDUN privacy threats modelling methodology, Available at: <https://linddun.org/linddun.php#> Last accessed on 17 April 2019.

Table 10 shows examples of mitigation strategies proposed in LINDDUN, showing an example related to the protection of identifiers (which is related to the identifiability and linkability of entities in a system).

TABLE 10 – EXAMPLE OF MITIGATION ACTIONS PROPOSED IN LINDDUN

Mitigation Strategy		Privacy Enhancing Techniques (PETs)
Protect ID	Pseudonyms	Privacy enhancing identity management system, User-controlled identity management system
	Attributes	Privacy preserving biometrics Private authentication
	Properties	Anonymous credentials (single show, multishow)

The LINDDUN website provides a catalogue of mitigation strategies and associated PETs. The catalogue should be considered as a living repository.

2.2.3 HOEPMAN DESIGN STRATEGIES

Privacy design strategies have been proposed¹⁹. They have been included in the guidance part of ISO/IEC 27550 (Privacy engineering for system lifecycle processes) and will be useful in a design process.

TABLE 11 – PRIVACY ENGINEERING DESIGN STRATEGIES

Design strategy		Description	Privacy control examples
Data oriented strategies	Minimize	Limit as much as possible the processing of PII	Selection before collection, Anonymization
	Separate	Distribute or isolate personal data as much as possible, to prevent correlation	Logical or physical separation; Peer-to-peer arrangement, Endpoint processing
	Abstract	Limit as much as possible the detail in which personal data is processed, while still being useful	Aggregation over time (used in smart grids), Dynamic location granularity (used in location-based services), k-anonymity
	Hide	Prevent PII from becoming public or known.	Encryption, Mixing, Perturbation (e.g. differential privacy, statistical disclosure control), Unlinking (e.g. through pseudonymization), Attribute based credentials
Process oriented strategies	Inform	Inform PII principals about the processing of PII	Privacy icons, Layered privacy policies, Data breach notification
	Control	Provide PII principals control over the processing of their PII.	Privacy dashboard, Consent (including withdrawal)
	Enforce	Commit to PII processing in a privacy friendly way, and enforce this	Sticky policies and privacy rights management, Privacy management system, Commitment of resources, Assignment of responsibilities
	Demonstrate	Demonstrate that PII is processed in a privacy friendly way.	Logging and auditing, Privacy impact assessment, Design decisions documentation

¹⁹ DANEZIS G., DOMINGO-FERRER J., HANSEN M., HOEPMAN J.-H., LE MÉTAYER D., TIRTEA R. et al. ENISA Report, Privacy and Data Protection by Design — from policy to engineering. December 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

2.2.4 OASIS PRIVACY MANAGEMENT REFERENCE MODEL METHODOLOGY (PMRM)

OASIS-PMRM²⁰ is a methodology for privacy operationalisation. PMRM will be replaced by the new standard under development: ISO/IEC 27561 (POMME: privacy operationalisation model and method for engineering):

- the method involves the description of application use cases;
- the method is iterative, with each iteration including three steps as showed in Table 12,
 - inventory of information,
 - specification of privacy controls, and
 - specification of functions and mechanisms to support privacy controls;
- at the end of one iteration, a compliance assessment (e.g., involving a privacy impact assessment based on ISO/IEC 29134) is applied to validate whether the privacy risks are suitably managed.

TABLE 12 – OASIS-PMRM OR POMME STEPS IN ONE ITERATION

Steps	Activities
Inventory of information	Participant identification
	System and business process identification
	Domains and owner's identification
	Intro-domain roles and responsibilities identification
	Touch points identifications
	Data flows identification
	PII identification
Specification of privacy controls	
Specification of functions and mechanisms to support privacy controls	

In the whole method, engineers must agree on the privacy principles and properties to operationalise. Table 13 shows the various taxonomies and input that can guide privacy engineering:

- the list of privacy principles can be based on ISO/IEC 29100. Other references can be used such as the OECD principles, or GDPR.
- possible security and privacy properties, based on the CIA triad and the privacy protection goals of ULD²¹.
- possible privacy engineering objectives²², and
- concepts that can guide the engineer based on the NIST privacy framework²³:

²⁰ ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS) PRIVACY MANAGEMENT REFERENCE MODEL AND METHODOLOGY. (PMRM), Version 1.0. July 2013, updated May 2016. <http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.pdf>

²¹ HANSEN M., JENSEN M., ROST M. "Protection Goals for Engineering Privacy"; in 2015 International Workshop on Privacy Engineering (IWPE). <http://ieee-security.org/TC/SPW2015/IWPE/2.pdf>

²² 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

²³ NIST privacy framework: a tool for improving privacy through enterprise risk management, version 1.0, January 2020. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

- it includes the 5 concepts of the NIST cybersecurity framework (or ISO/IEC 27110): identify, protect, detect, respond and recover,
- it includes specific concepts for the security protection of privacy related assets: protect-p, detect, respond, recover, and
- it finally includes specific concepts for privacy protection: identify-p, govern-p, control-p, communicate-p.

TABLE 13 – ISO/IEC 29100 PRIVACY FRAMEWORK PRINCIPLES

ISO/IEC 29100 privacy framework		Consent and choice
		Purpose legitimacy and specification
		Collection limitation
		Data minimization
		Use retention and disclosure limitation
		Accuracy and quality
		Openness
		Transparency and notice
		Individual participation and access
		Accountability
		Information security
		Privacy compliance.
Security and privacy protection goals	Security	Confidentiality
		Integrity
		Availability
	Privacy	Unlinkability
		Transparency
		Intervenability
Privacy engineering		Predictability
		Manageability
		Disassociability
NIST privacy framework	Cybersecurity risks	Identify
		Protect
		Detect
		Respond
		Recover
	Cybersecurity related privacy events	Protect-P
		Detect
		Respond
		Recover
	Privacy risks	Identify-P
		Govern-P
		Control-P
Communicate-P		

Once the method has been applied, a number of privacy capabilities should have been defined. Table 14 shows the privacy capability taxonomy proposed by OASIS-PMRM.

TABLE 14 – OASIS-PMRM PRIVACY CAPABILITIES TAXONOMY

Capability		Purpose	Description
Core policy capabilities	Agreement	Manages and negotiates permissions and rules	Defines and documents permissions and rules for the handling of PII based on applicable policies, data subject preferences, and other relevant factors; provides relevant Actors with a mechanism to negotiate, change or establish new permissions and rules; expresses the agreements such that they can be used by other services
	Usage	Controls PII use	Ensures that the use of PII complies with the terms of permissions, policies, laws, and regulations, including PII subject to information minimization, linking, integration, inference, transfer, derivation, aggregation, anonymization and disposal over the lifecycle of the PII
Privacy assurance capabilities	Validation	Ensures PII quality	Evaluates and ensures the information quality of PII in terms of accuracy, completeness, relevance, timeliness, provenance, appropriateness for use and other relevant qualitative factors
	Credential certification	Ensures appropriate management of credentials	Ensures that the credentials of any actor, domain, system, or system component are compatible with their assigned roles in processing PII and verifies their capability to support required privacy controls in compliance with defined policies and assigned roles.
	Enforcement	Monitors proper operation, responds to exception conditions and reports on demand evidence of compliance where required for accountability	Initiates monitoring capabilities to ensure the effective operation of all services. Initiates response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures. Records and reports evidence of compliance to stakeholders and/or regulators. Provides evidence necessary for accountability.
	Security	Safeguards privacy information and operations	Provides the procedural, organizational and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PII; makes possible the trustworthy processing, communication, storage and disposition of PII; ensures that the operational functionalities provided by other Services are protected to maintain their reliability and trustworthiness
Presentation and lifecycle capabilities	Interaction	Provides Information presentation and communication functionality	Provides generalized interfaces necessary for presentation, communication, and interaction of PII and relevant information associated with PII, encompassing functionality such as user interfaces, system-to-system information exchanges, and agents
	Access	Enables viewing and proposing changes to PII	Enables PII principals, as required and/or allowed by permission, policy, or regulation, to review their PII that is held or processed within a domain and to propose changes, corrections or deletion for their PII

2.3 SELECTION OF STANDARDISATION WORK ON SECURITY AND PRIVACY

A selection of standards is made, and their roles are explained. Note that many standards are not directly accessible because they have to be purchased. However,

- It is possible to have a look to the scope, introduction, terms and definition and standard structure²⁴,
- Several standards are freely available²⁵, and
- Lots of material are available on the web.

2.3.1 ISO/IEC 27001 — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS

TABLE 15 – ISO/IEC 27001 ISMS REQUIREMENTS

Reference	https://www.iso.org/standard/54534.html
Status	Public
Scope	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
Comment	Could be useful in Interconnect if an information system is developed in the project.
InterConnect position	Not a main reference in InterConnect work

2.3.2 ISO/IEC 27002 — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

TABLE 16 – ISO/IEC 27002 INFORMATION SECURITY CONTROLS

Reference	https://www.iso.org/standard/54533.html
Status	Public New edition is currently at working draft level.
Scope	ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: <ol style="list-style-type: none"> 1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; 2. implement commonly accepted information security controls; 3. develop their own information security management guidelines.

²⁴ <https://www.iso.org/obp/ui/#home>

²⁵ <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

Comment	<p>Could be useful in Interconnect if an information system is developed in the project. A new edition is underway that could have an impact on privacy standards (including 27701). It will use different control taxonomies:</p> <ul style="list-style-type: none"> • Main taxonomy: physical controls, people controls, organisational controls and technology controls. • Taxonomy 2: preventive, detective, corrective • Taxonomy 3: confidentiality, integrity, availability • Taxonomy 4: identify, protect, detect, respond, recover
InterConnect position	Not a main reference in INTERCONNECT work

2.3.3 ISO/IEC 27005 — INFORMATION SECURITY RISK MANAGEMENT

TABLE 17 – ISO/IEC 27005 INFORMATION SECURITY RISK MANAGEMENT

Reference	https://www.iso.org/standard/75281.html
Status	Public
Scope	<p>ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.</p>
Comment	<ul style="list-style-type: none"> • The standard can also be used for other systems than information security systems • The standard is very generic so that it can be used with specific variants. For instance, the French eBios standard specialises ISO/IEC 27005 • It does not cover privacy
InterConnect position	Should be a reference in InterConnect work. It has been included in the Annex III template as a choice to be made by pilots.

2.3.4 ISO/IEC 27110 (EX 27101) — CYBERSECURITY FRAMEWORK DEVELOPMENT GUIDELINES

TABLE 18 – ISO/IEC 27101 CYBERSECURITY FRAMEWORK DEVELOPMENT GUIDELINES

Reference	https://www.iso.org/standard/72435.html
Status	Current version is at committee draft level. Publication will take place this year.
Scope	<p>The goal of the ISO/IEC 27101 is to ensure a minimum set of concepts are used to define cybersecurity frameworks to help ease the burden of cybersecurity framework creators and cybersecurity framework users.</p> <p>As this document limits itself with a minimum set of concepts, its length is kept to a minimum on purpose.</p> <p>This document is not intended to supersede or replace the requirements of an ISMS given in ISO/IEC 27001.</p> <p>The principles of this document are as follows:</p> <ul style="list-style-type: none"> • Flexible - to allow for multiple types of cybersecurity frameworks to exist; • Compatible - to allow for multiple cybersecurity frameworks to align; and • Interoperable – to allow for multiple uses of a cybersecurity framework to be valid.

Comment	This framework can be extended to privacy with the NIST privacy framework. The energy sector is currently working on mapping the security needs to the NIST Framework. This work is done within IEC, as well as in a joint working group with ISO/IEC JTC1 IoT (Internet of things)
InterConnect position	Should be a reference in InterConnect work. It has been included in the Annex III template as a choice to be made by pilots.

2.3.5 ISO/IEC 27400 (EX-27030) — SECURITY AND PRIVACY GUIDELINES FOR IOT

TABLE 19 – ISO/IEC 27400 SECURITY AND PRIVACY GUIDELINES FOR IOT

Reference	https://www.iso.org/standard/75281.html
Status	Is as committee draft level
Scope	This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.
Comment	Document is viewed as a complement to ISO/IEC 30141 IoT reference architecture. Note that since ISO/IEC 30141 is undergoing a significant change, that may cause a restructuring of this standard. Document includes an ecosystem viewpoint Standards takes a risk orientation approach, that leads to the definition of a list of security controls and of a list of privacy controls Trialog is co-editing this standard.
InterConnect position	InterConnect should be aligned with ISO/IEC 27400. Contributions to the standard have been made by InterConnect, in particular on the need to have privacy controls related to the enforcement of privacy preferences. InterConnect will continue to contribute to ISO/IEC 27402. The list of controls will be made available to the pilots when they carry out the security and privacy risk analysis activities

2.3.6 ISO/IEC 27402 — IOT SECURITY AND PRIVACY – DEVICE BASELINE REQUIREMENTS

TABLE 20 – ISO/IEC 27402 – IOT SECURITY AND PRIVACY – DEVICE BASELINE REQUIREMENTS

Reference	https://www.iso.org/standard/80136.html
Status	Is a committee draft level
Scope	This document provides baseline requirements for IoT devices to support information security and privacy controls. This document covers IoT devices that have a network interface
Comment	This standard is moving forward very rapidly. One of the editors is French, and it will therefore be influential in future IoT systems certification schemes.
InterConnect position	InterConnect should be aligned with ISO/IEC 27402. Contributions to the standard have already been made by InterConnect (e.g. requirements on device sanity check). InterConnect will continue to contribute to ISO/IEC 27402.

2.3.7 ISO/IEC 27403 — IOT SECURITY AND PRIVACY – GUIDELINES FOR IOT-DOMOTICS

TABLE 21 – ISO/IEC 27403 IOT SECURITY AND PRIVACY – GUIDELINES FOR IOT DOMOTICS

Reference	https://www.iso.org/standard/78702.html
Status	Is at working draft level
Scope	This document provides guidelines to analyze security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.
Comment	<p>The document is currently structured as follows:</p> <ul style="list-style-type: none"> • Security and privacy concerns • Guidelines to assess risks of IoT domotics • Guidelines to design security and privacy of IoT domotics • Guidelines to implement security and privacy of IoT domotics <p>The document also includes an annex with six use cases: entertainment, electrical appliance control, monitoring and security system, care service, energy management and car video communication</p>
InterConnect position	InterConnect will be influential in the shaping of ISO/IEC 27403 in terms of guidelines and in terms of use cases.

2.3.8 ISO/IEC 27550 — PRIVACY ENGINEERING FOR SYSTEM LIFE CYCLE PROCESSES

TABLE 22 – ISO/IEC 27550 - PRIVACY ENGINEERING FOR SYSTEM LIFE CYCLE PROCESSES

Reference	https://www.iso.org/standard/72024.html
Status	Public
Scope	<p>This document provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes. It describes:</p> <ul style="list-style-type: none"> • the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and • privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design. <p>The intended audience includes engineers and practitioners who are involved in the development, implementation or operation of systems that need privacy consideration, as well as managers in organizations responsible for privacy, development, product management, marketing, and operations.</p>
Comment	Trialog was the main editor this standard, which was the direct outcome of the PRIPARE support action on privacy-by-design that ran from 2014 to 2016.
InterConnect position	This document will be used by InterConnect (the entire annex IV is based on the standard)

2.3.9 ISO/IEC 27556 — USER-CENTRIC FRAMEWORK FOR THE HANDLING OF PII BASED ON PRIVACY PREFERENCES

TABLE 23 – ISO/IEC 27556 USER-CENTRIC FRAMEWORK FOR THE HANDLING OF PII BASED ON PRIVACY PREFERENCES

Reference	https://www.iso.org/standard/71674.html
Status	Is currently at committee draft level

Scope	This document provides a user-centric framework for PII handling based on privacy preferences
Comment	This standard creates a specific role: the privacy preference administrator which interacts with citizens and operates a privacy preference management capability. The privacy preference administrator could be a data controller or a service provider. The concept of privacy preference management capability will be particularly important in data space marketplaces.
InterConnect position	InterConnect will work in synergy with OpenDei to contribute to and align with ISO/IEC 27556

2.3.10 ISO/IEC 27561 — PRIVACY OPERATIONALISATION MODEL AND METHOD FOR ENGINEERING (POMME)

TABLE 24 – ISO/IEC 27561 — PRIVACY OPERATIONALISATION MODEL AND METHOD FOR ENGINEERING (POMME)

Reference	Not yet available
Status	Is currently under ballot
Scope	This specification provides a model and method to operationalise privacy principles and privacy controls. It includes the following elements: <ul style="list-style-type: none"> • a method for capturing and organizing essential information necessary to define, scope and analyse a PII operational use case • a taxonomy, enabling more effective understanding and integration of interdependent privacy control functionality, particularly in complex use cases • an ontological structure of capabilities (non-normative) to help privacy engineers to categorize and organize privacy control functionality • concepts critical for the analysis of networked, interdependent applications, such as data flows, domains, domain owners, sources of PII, and policy associations • the selection of technical and procedural mechanisms necessary to operationalise privacy controls • support for software-based tools to simplify the collection, editing and lifecycle management of information and data relevant to the privacy aspects of an application.
Comment	Trialog will be a co-editor of this standard. It is basically the adaptation of OASIS-PMRM so that it will be aligned with ISO standards
InterConnect position	The use case approach will be useful to the construction of InterConnect pilots security and privacy solutions.

2.3.11 ISO/IEC 27570 — PRIVACY GUIDELINES FOR SMART CITIES

TABLE 25 – ISO/IEC 27570 PRIVACY GUIDELINES FOR SMART CITIES

Reference	https://www.iso.org/standard/71678.html
Status	Final version will go under publication in 2020
Scope	The document takes a multiple agency as well as a citizen centric viewpoint. It provides guidance on smart city ecosystem privacy protection, on how standards can be used at a global level and at an organizational level for the benefit of citizens, and on processes for smart city ecosystem privacy protection. This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

Comment	<p>Trialog is the main editor of this standard. It contains four main sections:</p> <ul style="list-style-type: none"> • a section on privacy in smart cities • a section providing guidance on smart city ecosystems privacy protection • a section on standards for smart city ecosystems privacy protection • a section on processes for smart city ecosystems privacy protection, including five processes: the governance process, the data management process, the risk management process, the engineering process and the citizen engagement process. <p>The annex includes an example of ecosystem privacy plan</p>
InterConnect position	<p>InterConnect works on a security and privacy plan is based on this standard (see annex III), which it extends to cover security. The resulting work of InterConnect could perhaps be promoted to a new standard</p>

2.3.12 ISO/IEC 27701 — EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS AND GUIDELINES

TABLE 26 – ISO/IEC 27701 EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS AND GUIDELINES

Reference	https://www.iso.org/standard/71670.html
Status	Public
Scope	<p>This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.</p> <p>This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.</p> <p>This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.</p>
Comment	Is the most important standard for organisations that have to manage an information system that include personal data.
InterConnect position	The privacy controls listed in the standard are used as a reference in InterConnect work. While the standards is focusing on information systems, the taxonomy will be useful in general. Several tables in the Interconnect template (see Annex IV) follow the 27701 privacy control taxonomy.

2.3.13 ISO/IEC 29134 — GUIDELINES FOR PRIVACY IMPACT ASSESSMENT

TABLE 27 – ISO/IEC 29134 GUIDELINES FOR PRIVACY IMPACT ASSESSMENT

Reference	https://www.iso.org/standard/62289.html
Status	Public
Scope	<p>ISO/IEC 29134:2017 gives guidelines for</p> <ul style="list-style-type: none"> • a process on privacy impact assessments, and • a structure and content of a PIA report. <p>It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.</p> <p>ISO/IEC 29134:2017 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.</p>
Comment	Is indispensable for privacy risk assessment

InterConnect position	Should be a reference in InterConnect work, along with ISO/IEC 27005.
-----------------------	---

2.3.14 ISO 31700 — PRIVACY BY DESIGN FOR CONSUMER GOODS AND SERVICES

TABLE 28 – ISO/IEC 31700 PRIVACY-BY-DESIGN FOR CONSUMER GOODS AND SERVICES

Reference	https://www.iso.org/standard/76772.html
Status	Is currently at working draft level
Scope	Specification of the whole of product design lifecycle process to provide consumer goods and services that meet consumers' processing privacy needs as well as the personal privacy requirements of Data Protection. In order to protect consumer privacy the functional scope includes security in order to prevent unauthorized access to data as fundamental to consumer privacy, and consumer privacy control with respect to access to a person's data and their authorized use for specific purposes. The process is to be based on the ISO 9001 continuous quality improvement process and ISO 10377 product safety by design guidance, as well as incorporating privacy design JTC1 security and privacy good practices, in a manner suitable for consumer goods and services
Comment	<p>Trialog is an active contributor to this standard. While this standard is challenging to build because it requires multidisciplinary convergence, it is likely that it will be the most important standard in the future.</p> <p>The current version includes about 50 requirements, structured according to a lifecycle vision:</p> <ul style="list-style-type: none"> • Design • Development • Release • Support • Retirement <p>The next version (Committee Draft) will probably take a different structure:</p> <ul style="list-style-type: none"> • Empowerment • Transparency • Lifecycle • Ecosystem • Responsibility • Institutionalisation
InterConnect position	Should be a reference in InterConnect work. The list of requirements can be used as a reference during the pilot security and privacy risk analysis work. Further Interconnect may want to contribute through Trialog and the PDP4E H2020 liaison to PC317.

2.3.15 IEC 62443 SERIES

IEC-62443 is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach to cybersecurity for industrial systems. Every stage and aspect of industrial cybersecurity is covered, from risk assessment through operations.

Using the techniques described in IEC 62443, industrial stakeholders can assess the cybersecurity risks to each system and decide how to address those risks. Recognizing that not every system is equally critical, IEC 62443 defines five security levels (SLs): from SL 0 (no security) to SL 4 (resistant against nation-state attacks).

Specific security requirements are defined for each security level so each industrial system will have the right security, protecting uptime, safety, and intellectual property. All parties in the industrial ecosystem benefit from having clear expectations: asset owners and operators, systems integrators, equipment and service providers, and regulators.

2.4 OTHER REFERENCE DOCUMENTS

2.4.1 NIST 7628 – GUIDELINES FOR SMART GRID CYBER-SECURITY

The NIST guidelines for smart grid cyber-security²⁶ is a reference for cybersecurity and privacy. It consists of three volumes. The first volume provide guidelines for security, architecture and high-level requirements. The document is mature and complete. It can be used as a knowledge source for Interconnect security risk analysis. In particular section 3 of the first volume provides a list of high-level security requirements. The second volume provides information on various types of use cases (smart grid use case, electric vehicles). The last volume provides a landscape

2.4.2 NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity framework²⁷ provides a common language for cybersecurity organised around five functions (identify, protect, detect, respond, recover). When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The framework can be considered as a cybersecurity knowledge repository. It comes with a comprehensive categories and subcategories – which are discrete outcomes – for each function, and matches them with example Informative references such as existing standards, guidelines, and practices for each subcategory. The framework can be used to guide the risk management process and ease integration in the system lifecycle process. It has been used to build ISO/IEC 27110 guidelines for cybersecurity framework.

2.4.3 NIST PRIVACY FRAMEWORK

The NIST privacy framework²⁸ extends the NIST cybersecurity framework with further functions (identify-P, govern-P, Control-P, Communicate-P, Protect-P). The framework can therefore be considered as a privacy protection knowledge repository. NISTIR 8200 - Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)

²⁶ <https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final>

²⁷ <https://www.nist.gov/cyberframework>

²⁸ <https://www.nist.gov/privacy-framework>

2.4.4 NISTIR 8062 - AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS (FINAL AND DRAFT)

This document²⁹ has been used as input to ISO/IEC 27550 (privacy engineering for system lifecycle processes). It provides an introduction to how systems engineering and risk management can be used. It explains the distinctions between security and privacy, introduces a set of privacy engineering objectives—predictability, manageability, and disassociability, and finally introduces a privacy risk model to conduct more consistent privacy risk assessments based on the likelihood that an operation performed by a system would create a problem for individuals when processing PII—a problematic data action—and the impact of the problematic data action should it occur.

2.4.5 PRIPARE PRIVACY AND SECURITY BY DESIGN METHODOLOGY HANDBOOK

PRIPARE was the main support action funded by the European Commission on privacy-by-design. The result was the publication of the PRIPARE handbook³⁰ that has been used as input to ISO/IEC 27550 (privacy engineering for system lifecycle processes). The methodology includes eight phases (environment & infrastructure, analysis, design, implementation, verification, release and maintenance. of the PRIPARE methodology. It also includes a privacy and security management analysis (PSMA) template which can be used for the work products of the processes.

2.4.6 MICROSOFT DATA PROTECTION/PRIVACY MAPPING PROJECT

Microsoft Data Protection/Privacy Mapping³¹ is an open source tool that maps data projection regulations against ISO/IEC 27701 standard. The project aims to provide the global privacy engineering community a shared understanding of how the ISO/IEC 27701 controls relate to global regulatory requirements around the world. Figure 10 shows the GDPR tab data correlated with ISO 27701 sections. Figure 11 shows the resulting dataset. Several legislations are available (Australia, Brazil, Californica CCPA, Canada, Hong Kong, NIST privacy framework, USA, Singapore, South Korea, Turkey...). Note that PDP4E has now a liaison with ISO PC 317 which is developing ISO 31700 (privacy-by-design for consumer goods and services). We will investigate the possibility to contribute such a mapping. It should also be noted that, in any case, ISO/ICT 27701 provides a set of privacy controls, which do not provide an exhaustive mapping to privacy regulations which deal as well with other concepts (e.g. privacy principles, data subject rights).

²⁹ <https://csrc.nist.gov/publications/detail/nistir/8062/final>

³⁰ https://ipen.trialog.com/images/ipen/a/a1/PRIPARE_Methodology_Handbook_Final_Feb_24_2016.pdf

³¹ <http://aka.ms/dpmap>



FIGURE 10. EXAMPLE OF VISUAL MAPPING OF THE MICROSOFT DATA PROTECTION/PRIVACY MAPPING TOOL³²

	A	B	C	D	E
1	id	section	body	hyperlink	isolinks
2	5	5	Principles relating to processing of personal data	https://eur-lex.europa.eu/eli/reg/	
3	5.1	5.1			
4	5.1.a	5.1.a	Article(5)(1)(a): Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulne		7.2.2;8.2.2
5	5.1.b	5.1.b	Article(5)(1)(b): Personal data shall be: (b) collected for specified, explicit and legitimate purposes		7.2.1;7.4.1
6	5.1.c	5.1.c	Article(5)(1)(c): Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they a		7.4.1;7.4.4
7	5.1.d	5.1.d	Article(5)(1)(d): Personal data shall be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");		7.3.6;7.4.3
8	5.1.e	5.1.e	Article(5)(1)(e): Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the		7.4.4;7.4.5
9	5.1.f	5.1.f	Article(5)(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").		6.10.2.1;6.15.1.3;7.
10	5.2	5.2	Article(5)(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")		
11	6	6	Lawfulness of processing	https://eur-lex.europa.eu/eli/reg/	
12	6.1	6.1			
13	6.1.a	6.1.a	Article(6)(1)(a): Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;		7.2.2
			Article(6)(1)(b): Processing shall be lawful only if and to the extent that at least one of the following applies: (b) processing is necessary for the performance of a contract to which the data subject is		

FIGURE 11. EXAMPLE OF ASSOCIATED MICROSOFT DATA PROTECTION/PRIVACY MAPPING DATASET³³

³² <https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard>

³³ <https://github.com/microsoft/data-protection-mapping-project/blob/master/src/assets/database.xlsx>

3. SECURITY AND PRIVACY PRINCIPLES

3.1 RATIONALE FOR THE PRINCIPLES

3.1.1 VALUE OF CURRENT WORK ON SECURITY AND PRIVACY

The previous section has provided a comprehensive overview of the projects and standards. We can observe the following:

- There is a need to focus on an overall ecosystem viewpoint (section 2.1)
- There are commonalities on methodologies (section 2.2)
- The overview on standardisation work (section 2.3) and other references (section 2.4) show a wealth of reference documents. In particular
 - ISO/IEC 27570 (privacy guidelines for smart cities) is the only reference that deals with ecosystem practice, but it only focuses on privacy. There are no known work on ecosystem security and privacy plans, and Interconnect can be the opportunity to provide a contribution on such plans³⁴;
 - Many references can be suggested in security and privacy plan template to help pilots finalising those they wish to use. For instance ISO/IEC 29134 (privacy impact assessment guidelines) can be a suggestion for privacy. These references are therefore listed as suggestions in the security and privacy plan template (defined in annex III).
 - Many references can be used as optional as they can depend on each pilot specific need. They should therefore be considered as part of a security and privacy practice knowledge repository that is consulted when pilots design their security and privacy solutions.

3.1.2 CONTRIBUTING TO SECURITY AND PRIVACY FOR ICT ECOSYSTEMS

Interconnect is part of the DEI FA LSP wave 2 and 3 of the European Commission. It was preceded by the IoT FA LSP wave 1 that is under completion. It includes LSP projects such as Synchronicity, Autopilot, Monica, Activage, IoF2020, and support actions such as Create-IoT and U4IoT. Wave 2 and 3 includes LSP projects on agriculture (e.g. Atlas, Demeter), energy (e.g. Interconnect), eHealth (e.g., GateKeeper, PHArA-On) and support actions such as OpenDei.

All the LSP are dealing with “small ICT ecosystems”. Practices on security and privacy need to be put in place with several perspectives:

- A: addressing the specific security and privacy objectives of the project, for instance using or implementing a block chain technology to implement smart contracts;
- B: addressing the security and privacy requirements of the pilot operation (e.g., GDPR compliance when personal data is collected); and

³⁴ This analysis was made when Interconnect proposal was made and led to the proposal to define security and privacy plans for ecosystems.

- C: anticipating the security and privacy requirements of future deployment (e.g., compliance with future practices such as cybersecurity certification).

This deliverable addresses perspectives B and C with the following objectives:

- Create a practice that reuse experience collected in previous LSPs
- Check whether the resulting practice can be promoted for synergy. This can be done at the support action level (e.g., OpenDei) and at the standardisation level (e.g., a work item on ecosystem security and privacy plans)

3.1.3 RESULTING PRACTICES FOR ICT ECOSYSTEMS

Two practices have been identified:

- A **policy framework analysis** which provides a high-level analysis of each pilot. The analysis includes a trust view from a socio-economical and business perspective, an engagement view covering ethics, standards, legislation and contracts, and a security and risk analysis view. This practice was initiated during the IoT FA LSP wave 1 by the Create-IoT support action³⁵. It allowed the pilots to reflect on aspects which are important at deployment level. We believe that the LSP and the further waves should continue this reflection work. Interconnect plans to reuse the Create-IoT template, to carry the analysis at the end of its pilots, and to communicate the result to the OpenDei support action.
- A **security and privacy plan analysis** which provides an operational analysis of each pilot. While this practice was carried out in an ad-hoc fashion during the IoT FA LSP wave 1, the policy framework analysis work showed that security and privacy risk analysis exhibit many common practices. Interconnect plans to focus on creating a common synergistic practice and report it to OpenDei as an LSP best practice. It is also expected that the resulting practice can be standardised.

These two practices form the two security and privacy principles which Interconnect will focus on. They are elaborated in the next two sections (3.2 and 3.3).

3.2 PRINCIPLE 1: POLICY FRAMEWORK ANALYSIS

A policy framework analysis will be provided by each pilot, including

- a trust analysis of the pilot ecosystem, covering a socio-economical perspective, business perspective and an analysis of the desired properties (security, safety, reliability, connectivity, resilience, availability...). The template provided by Create-IoT can be used (see Table 4)
- an engagement analysis of the pilot ecosystem, covering engagement on ethics, standards, legislation and contracts. The template provided by Create-IoT can be used (see Table 5)
- a security and privacy engineering approach. The template provided by Create-IoT can be used (see Table 6)

³⁵ IoT Policy Framework Evaluation and Final IoT Policy Framework. Create-IoT project Deliverable D5.2 December 2019. https://european-iot-pilots.eu/wp-content/uploads/2020/06/D05_02_WP05_H2020_CREATE-IoT_Final.pdf

The following is proposed to Pilots

- a first common understanding will be gained in a specific task 2.3 webinar³⁶, prior the starting of the pilot operations
- during the pilots, the operations will be monitored,
- an analysis will be provided by the pilots when enough experience has been gained. To this end a specific workshop to be organised in task 5.3 towards the end of the pilots using the template in annex II.

3.3 PRINCIPLE 2: SECURITY AND PRIVACY PLAN

- A security and privacy plan will be specified by each pilot:
 - the construction of the plan and its execution will be based on the following common process
 - an initial questionnaire will be filled out by each pilot,
 - a webinar will be organised to explain the process³⁷,
 - a template will be provided (annex III),
 - a workshop will be carried out with each pilot to explain how to create specific security and privacy plans,
 - the pilots will finalise their own security and privacy plans,
 - a second workshop will be carried out focusing on the pilot specific security and risk analysis (using Annex IV guidance).
- the content of the plan is based on the ISO/IEC 27570 ecosystem privacy plan, extended to include security. A template is proposed in Annex II, including
 - a governance management plan
 - a data management plan
 - a risk management plan
 - an engineering management plan
 - a citizen engagement plan

³⁶ This seminar was held on November 3rd, 2020 (see annex VI for the slides)

³⁷ This webinar was carried out on November 3rd, 2020. See Annex VI for the slides.

4. IMPLEMENTATIONS GUIDELINES

4.1 SPOCS (SECURITY AND PRIVACY POLICIES COMPLIANCE SOLUTION)

4.1.1 DEFINITION OF A SPOCS

The Interconnect ecosystem concerns IoT systems deployed in residential environment as well as large industrial systems like smart-cities and smart-grid context. This creates some unique cybersecurity issue since though IoT has been widely applied worldwide, many IoT devices, communications and platforms lack security and privacy considerations, which may pose security and privacy risks.

Due to the long industrial chain and a large number of stakeholders involved, it is necessary to sort out the roles, identify risks during the lifecycle and put forward proposals for resolving security and privacy issues in ecosystems such as InterConnect. This work aims to provide tools to define guidelines to manage, analyse and treat security and privacy risks and challenges.

This document's goal is to define methods and tools to help defining technical and management solutions to cybersecurity and privacy issue during the Interconnect pilots. The SPOCS is a global solution to create a **Security and Privacy Plan** that should be used during the project to manage all aspects of this issue.

The SPOCS will cover:

- **Governance management:** Governance of a project is essential for industrial projects and should be considered even in experiments such as Interconnect Pilots, the responsibility and role in the cybersecurity and privacy systems
- **Data Management:** Data Management is essential for privacy needs, the PII must be identified and treated with care in particular in an ecosystem that will need to exchange such data for its applications
- **Risk Management:** The methodology and process to conduct a risk analysis as well as the regularity of such analysis must be stated and projected at the beginning of the project
- **Engineering Management:** The engineering tools and methods to ensure cybersecurity should be defined. This category is most likely to evolve as a result of further developments regarding cybersecurity and privacy technologies
- **Citizen Engagement:** The use of PII at such a large scale with a great variety of participants and stakeholder makes citizen engagement and users implication essential to evaluate the possibility in the data usage

This approach is unique since even if privacy and cybersecurity have a close bond, there is little work for a combined definition of such methodology considering both issues in a single document. As such the SPOCS foresees future works on such integration.

The SPOCS are destined for experimental ecosystems, a further expansion is needed for use of complete functional ecosystem.

4.1.2 INTEGRATING THE CONSORTIUM AND THE PILOTS NEEDS IN THE CREATION OF A SECURITY AND PRIVACY PLAN

The creation of a security and privacy plan requires the combination of two perspectives:

- A consortium perspective where pilots integrate and assess common innovations capabilities develop by the consortium.
- A pilot perspective where specific needs of a pilot (e.g., local regulation) must be taken into account.

Consequently, the content of all pilots' security and privacy plans must include considerations on the common innovation capabilities they are using. This means that in order to avoid duplicate efforts when the security and privacy plans are executed, some preliminary inputs should be provided to pilots. In particular a security and risk analysis of the common innovation capabilities should be provided to pilots.

4.1.3 PROCESS TO CREATE A SECURITY AND PRIVACY PLAN

SPOCS is a process to create a **Security and Privacy Plan (SPP)** for each pilot. This Plan should help the governance body to follow the work on cybersecurity and privacy in the project. During the realisation of the SPP, some decisions about responsibility, needs and methodology should be defined for the project.

To create the SPP, a workshop for each pilot should be organized. This workshop will aim to give a first understanding of the content of the SPP and to define the needs for cybersecurity and privacy of the pilot. It should also reuse input provided by the consortium on the security and privacy properties of the innovation capabilities that they are providing to the pilots.

At the end of this workshop, a report will be redacted between the security expert and the project team to generate a first version of the SPP. This first version will be confirmed by a second workshop to clarify the points still undefined if necessary.

The SPP is not a fixed document. It should be able to evolve during the project development and life in particular for experimental project such as Interconnect Pilots.

Major change in the pilot goals or technical choice should bring a review of the SPP to check its accordance with the current project definition and the future needs of the project.

4.2 CONTENT OF THE SECURITY AND PRIVACY PLAN

The SPP is based on a template (in annex III) that can will facilitate its creation. The plan is constructed with two perspectives:

- Serving the operation of the pilot, i.e., the security and privacy plan addresses the security and privacy risks of the pilot
- Addressing the needs of deployment beyond the project. This requires getting an understanding on what will be needed for such deployment.

Interconnect will focus on the first perspective during the operation of the pilot and reflects on the second perspective when it reflects on the policy framework analysis at the end of the pilot.

4.2.1 GOVERNANCE MANAGEMENT PLAN

The Governance Management plan describes governance scheme, objectives and governance body. It includes the following items:

- **Rules, legislations, applicable international standards:** Legislation include current regulation at the time of the pilot (e.g., GDPR) as well as legislation that will be in place beyond the project (e.g., cybersecurity act). It is directed by contractual schemes at the time of the pilot (e.g., grant agreement, consortium agreement, local pilots agreement) and beyond. Standards can be based on those listed in section 2. They can be specific to national needs (e.g., specific security risk methods in some countries.)
- **Governance body:** the SPP specifies the governance structure, the stakeholders involved and their role in the governance. In the case of a pilot, governance is simplified because all pilots are under the same H2020 contracts. Beyond the project, a specific body might have to be set up, either led by a public authority, or by a private organisation. This includes the identification of stakeholders in charge of security governance and of privacy governance. Because pilots are ecosystems, the governance body should include all the organizations participating to the operation of the ecosystem.
- **Organizations, organizations structure and responsibility:** the list of organizations of the ecosystem should be listed, their specific roles and responsibility should be specified. In the case of pilots, this includes the beneficiaries and the suppliers that will be involved in the pilot.
- **Rules and procedure:** in a complex ecosystem such as Interconnect pilot, the role and responsibility between each provider, user and other party should be clearly defined. This section should explain the operation of the governance body, statutes, meeting frequency and rules. In the case of pilots, provisions of the grant agreement, consortium agreement, and specific agreement should be used. Specific sections should be included if personal data is collected, requiring consent management capabilities.
- **Continual improvement:** a SPP might miss some important aspects or might need modification further to a modification of a pilot. An SPP modification is therefore needed through a continual improvement process (periodic review, or specific update upon request). Note that within the time frame of a pilot, it is not likely that the SPP will need modification. This will be however an important element of a SPP in a deployment beyond the project.

4.2.2 DATA MANAGEMENT PLAN

The Data Management plan extends the H2020 data management plan to the pilots. It includes the following

- **Pilot needs and resources for security and privacy data management:** the SPP describes the pilot needs in terms of resources. This includes both the security needs (e.g., business data IPR) and privacy needs (e.g., personal data protection). The SPP should

identify the persons responsible for the management of security and privacy (e.g., data controller, data processors). It should identify whether there are cases whether citizens data is collected. In this case resources to manage interactions with them must be identified

- **Data management process:** the SPP describes the process that will be implemented for data management, extending the data management plan. It identifies the various needs for data agreements, either consent management forms with citizens, or data sharing agreements with suppliers in the ecosystem.
- **Data description:** the SPP describes each data set, the date when collection is started and halted, it provides an identification, it categorizes the data (personal data, business data, or critical data for service provision), it describes the data the lifecycle (storage time, deletion process).
- **Data exchange:** the SPP describes the data flow between entities and stakeholders as well as the data access control chart between entities and persons
- **Data access monitoring:** the SPP describes the procedure to check data integrity and access authorisation. Note that beyond the project there could be requirements for auditing this capability.
- **Data registry:** the SPP explains how agreements are stored and managed. It manages and stores datasets or information on data sets, and it manages and stores information on consent managements (for personal data collection)

4.2.3 RISK MANAGEMENT PLAN

The risk management plan includes the following

- **Pilot needs and resources for security and privacy risk management:** the SPP identifies for each pilot application whether a privacy impact assessment is needed and whether a security risk analysis is needed. If the pilot uses common innovation capabilities of the project, the SPP indicates whether the capability is provided with information on its security and privacy risk.
- **Risk management process:** the SPP indicates the security risk analysis methodology and the privacy risk analysis methodology that is used. Interconnect will provide a template suggesting methodologies that it will support. This includes the use of STRIDE and of the NIST security framework for security threat analysis, the use of ISO/IEC 27005 for security risk analysis, the use of LINDDUN and the NIST privacy framework for privacy threat analysis, and the use of ISO/IEC 29134 for privacy impact assessment. The SPP also provides a schedule on when risk analysis is performed. Note that risk analysis is iterative and can be carried out several times, but since Interconnect is limited in time, each pilot will plan for one session that will take place prior to the final design of the system to be developed. The SPP identifies the template to be used for risk analysis. Interconnect will provide one, but pilots may wish to use their own template.

4.2.4 ENGINEERING MANAGEMENT PLAN

The engineering management plan includes the following

- **Pilot needs and resources for security and privacy engineering:** the SPP identifies for each pilot the security and privacy capabilities to be used, the competences needed and the persons to be allocated.
- **Engineering process:** the SPP indicates the methodology and process of development and engineering to ensure security and privacy of the application. It identifies the engineering process used (e.g., ISO/IEC/IEEE 15288 system life cycle processes), the security engineering approach used (e.g., NIST Framework (Identify, protect, detect, respond, recover)), the privacy engineering approach used (e.g., NIST Framework (Identify, control, govern, communicate, control), ISO/IEC 27550 privacy engineering for system lifecycles), ISO/IEC 27001/27002 and 27701. The SPP also provides a schedule on when privacy engineering activities take place. Note that engineering and risk analysis must run in a synchronised way, therefore the schedule should be compatible. In the case a pilot is using common innovation capabilities developed by the consortium, they should integrate in the schedule the activities to integrate these capabilities in the design of their pilot.

4.2.5 CITIZEN MANAGEMENT PLAN

The citizen management plan deals with citizen interactions (e.g., for personal data consent management) and citizen engagement needs (e.g., consulting citizen in the community to validate and/or make a decision concerning the ICT ecosystem). It includes the following

- **Pilot needs and resources for citizen management:** the SPP identifies for each pilot the needs for resources and competences either for interacting with citizens for consent management or for interaction with the citizens community for decision-making. This can involve public relation capability.
- **Engagement process:** the SPP plans and specifies the various cases when citizen must be engaged. This includes the specification of an interaction process with citizens in case where personal data is collected and where consent must be requested. The resulting SPP must detail the overall consent management process, including the specification of consent forms, activities for legal conformance verification, public relation to contact citizens, and the support for citizen information requests. The SPP can also include the specification of a citizen engagement process when consultations with the community is expected to decide on policies that have an impact on security and privacy, for instance whether it is accepted to deploy a community application that is collecting personal data.

5. CONCLUSION

This deliverable provides the Cybersecurity and Privacy framework, that we called Security and privacy Policies Compliance Solution (SPOCS). It includes the Security and Privacy Plan that comprises five sub-plans: 1) Governance Management Plan, 2) Data management Plan, 3) Risk management plan, 4) Engineering Management Plan, and 5) Citizen Engagement Plan.

The Security and Privacy Plan is being applied to pilots within the workshops. We assist pilots to secure better their systems of systems. We can clearly see that thanks to the questionnaires answered by the pilots in the first year of the project in March 2020, we help improve the security and privacy by design of their systems. Refinement of the plan will be done following the feedback and experience, and will be addressed in Task 5.3 “Applying practice for security and privacy policies compliance” and will be summarized in D5.3 “Security, cyber-security and privacy protection action plan and results”.

Annex I. QUESTIONNAIRE TEMPLATE SENT TO PILOTS: CYBERSECURITY AND PRIVACY EXPERTISE QUESTIONNAIRE

InterConnect H2020 Project WP T2.3 Cybersecurity and Privacy

NAME:
COMPANY:
Contact details (e-mail):

Use case Summary:

Which organization are participating in the use case? Which responsibility does each have about the data treatment?

Operators of Essential Services:

Others organizations:

What are the cyber security and privacy experiences of the pilot participants?

Cybersecurity and privacy experiences:
<ul style="list-style-type: none"> DPIA: Security Risk Analysis: Privacy by design: Security by design:

Is there's any cybersecurity or privacy measure already in place in the pilot which could be related to the project?

Already in place processes for cybersecurity:

Already in place processes for privacy:

Are there any cybersecurity or privacy measures planned for the pilot development?

Planned measures for cybersecurity:

Planned measures for privacy:

Annex II. POLICY FRAMEWORK TEMPLATES

These templates have been presented in a task 2.3 webinar to pilots³⁸. An analysis will be provided by the pilot when enough understanding has been gained by them.

Trust analysis template	
Socio-economical perspective	To be provided by pilot
Business perspective	To be provided by pilot
Properties (e.g., Security, Safety, Reliability, Connectivity, Resilience, Availability)	To be provided by pilot

Engagement analysis template	
Engagement on ethics	To be provided by pilot
Engagement on standards	To be provided by pilot
Engagement on legislation	To be provided by pilot
Engagement on contracts	To be provided by pilot

Security and privacy analysis template	
Risk management (use the Automat security and privacy risk analysis template)	To be provided by pilot
Designing security and privacy:	To be provided by pilot
Assuring security and privacy	To be provided by pilot

³⁸ Held on November 3rd, 2020. See annex VI for the slides

Annex III. SECURITY AND PRIVACY PLAN TEMPLATE

This template will be presented in a task 2.3 webinar to pilots. A workshop will be carried out with each pilot to work on the creation of the plan.

1			Security and Privacy Plan Context	
Application Name		Name of the application or Pilot developing the application		
Summary		Short summary of the Application (with a maximum of 280 char)		
Description		Extended description of the Application (text, images, etc.) : For example, define which use cases of the WP1 are implemented in the Application Identification of Pilot contribution (Data exchange, AI, Simulation....) and possibility to use INTERCONNECT building blocks (including the unified access control)		

2			Governance Management Plan	
Rules and legislation		Identify the applicable rules since governance management differs in countries: Industrial Rules GDPR Local Law Business Policy		
International Standards		Identify which International Standards should be followed by the application (see chapter 2)		
2.1			Governance Body	
Information Security Manager		Identify the person responsible for: ensuring that the information security management system conforms to the requirements of project security reporting on the performance of the information security management system to top management.		
Data Protection Officer		If Personal Identifiable Informations (PII) are used, define a Data Protection Officer responsible for the treatment		
Other roles		Identify if needed other role of the governance body		
2.2			Organisation responsibility	
Entity 1	Entity Name	Name of the participant organisation		
	Role	Role of the participant organisation		
	Address	Address of the participant organisation		
	Contact(s)	Name and email of the contact person(s)		
	Entity Type	Type of organization		

Structure of responsibility	Identify the structure of responsibility between organization for security and privacy purpose
2.3	Rules and procedure
Meetings	Describe the meeting rules for the governance body
Nomination	Describe the nomination procedure of the governance body
Publication of minutes	Describe the publication process of the minutes of the governance body meeting
2.4	Continual improvement
Meetings	Describe the meeting rules for the continual improvement evaluation? Meetings can be periodic (regular check) or called upon in case of incidents
Evaluation procedure	Describe the security and privacy evaluation procedure Note that an evaluation can take place after the 3rd workshop (where security and privacy analysis is carried out)

3	Data Management Plan³⁹
Interconnect data management plan is the first input	
3.1	Pilot needs and resources for security and privacy data management
Ownership of data	Identification of the owner(s) and right holders of data
PII Controller⁴⁰	Identification of the PII Controller(s) in the application context
PII Processors⁴¹	Identification of the PII Processors in the application context
PII Principals⁴²	Identification of the PII Principals in the application context
3.2	Data Management Process
3.2.1	Agreements
Agreement approach	Define the consent management approach in case of PII Define the data sharing agreement between the PII Controller and PII Processor Define the need for lawfulness processing (e.g., consent management between the PII Controller and PII principals). Define the IPR and confidentiality agreement
A or	Organizations
	Identification of the organizations concerned by the agreement

³⁹ The pilot may have two or more applications. The data management plan should be repeated for each application.

⁴⁰ 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

⁴¹ 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

⁴² ISO/IEC TR 27550 definition: Natural person to whom the personally identifiable information (PII) relates

	Agreement template	Define the agreement template: <ul style="list-style-type: none"> Contract (e.g., could be the consortium agreement, H2020 grant agreement) Note: one can state that he does not have access to the suppliers of a supplier (then there must be a clause in the template below to remind about responsibilities)
3.2.2	Data description	
Data 1	Dates for collection	Date when collection starts and ends
	Identification of data	Identification of the data
	Type of data	Identify if the data is: <ul style="list-style-type: none"> PII (Personally Identifiable Information) Business data Critical to service data
	Life Cycle	Identify the life cycle of the data : <ul style="list-style-type: none"> Storage time Deletion process
	Data description	Extended description of the data (text, images, etc.) or reference to a document
3.2.3	Data exchange	
	Data flow	Describe the data flow between entities and stakeholder
	Data access control chart	Describe the data access chart between entities and persons
3.2.4	Data access monitoring	
	Data access verification procedure	Describe the procedure to check the data integrity and access authorizations
3.2.5	Data registry	
	Registry of agreements	Explain how agreements are stored and managed
	Registry of data sets	List data sets and explains how they are stored and managed
	Registry of citizen consents	Manage citizen consents.

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	Identify if a security analysis is needed

analysis	
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	<p>Identify the security risk analysis methodology used:</p> <ul style="list-style-type: none"> • STRIDE <ul style="list-style-type: none"> ○ Security Properties: Authentication, Integrity, NonRepudiation, Confidentiality, Availability, Authorization ○ Security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege • NIST Security Framework (e.g., Identify, Protect, Detect, Respond, and Recover)
Schedule	<p>Specify the program of work (dates, deliverables)</p> <p>Each pilot will schedule meeting 3 (focusing on security and privacy risk analysis. See annex VI)</p>
Template	Identify the template used for risk analysis (Interconnect will supply one)
4.2.2	Privacy
Methodology	<p>Identify the privacy risk analysis methodology used:</p> <ul style="list-style-type: none"> • LINDDUN <ul style="list-style-type: none"> ○ Privacy properties: unlinkability, Anonymity, Plausible deniability, Undetectability, Confidentiality, Context-Awareness, and Consent Compliant ○ Privacy threats: Linkability, Identifiability, Non-Repudiation, Undetectability, Disclosure of information, Context unawareness, Consent, Non compliance • CNIL • NIST Privacy Framework (Identify, Govern, Control Communicate, and Protect) • ISO/IEC 29134
Schedule	<p>Specify the program of work (dates, deliverables)</p> <p>e.g. Position meeting 3 (security and privacy risk analysis. See annex VI)</p>
Template	Identify the template format used for risk analysis

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)</p> <p>Identify the common innovation capabilities that will be used (e.g. interoperability framework, access control, DLTs,...)</p>
Engineering process	Identify the methodology and process of development and engineering to ensure security and privacy of the application:

	Engineering: e.g., ISO/IEC/IEEE 15288 system life cycle processes Security engineering: e.g., NIST Framework (Identify, protect, detect, respond, recover) Privacy engineering: e.g., NIST Framework (Identify, control, govern, communicate, control), ISO/IEC 27550, ISO/IEC 27001/27002 and 27701
Schedule	Specify the program of work (dates, deliverables). This can include WP5 proposal on common innovation capabilities to be used by pilot Pilot feedback and agreement Consequently risk analysis Implementation

6 Citizen Management Plan	
Pilot needs and resources for engagement	Description of the citizen interaction and citizen engagement needs
Engagement process	Specify the interaction process. For instance, needs for consent vs legitimate interest Specify the engagement process for instance <ul style="list-style-type: none"> • 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? • Citizen consultation • Transparency; Describe the process for PII principals to access their data; Describe the process for users to send review and request about the application
Schedule	Specify the program of work (dates, deliverables)

Annex IV. SECURITY AND PRIVACY RISK ANALYSIS SUPPORT

Security threat analysis

TABLE 29 – STRIDE SECURITY THREATS

	Threat	Property	Property description
IoT systems security objectives expressed as threats to counter	Spoofing	Authentication	The identity of IoT entities or IoT users is established (or you are willing to accept anonymous entities).
	Tampering	Integrity	IoT data and system resources are only changed in appropriate ways by appropriate people.
	Repudiation	Nonrepudiation	IoT users cannot perform an action and later deny performing it.
	Information disclosure	Confidentiality	Data is only available to the IoT users intended to access it.
	Denial of Service	Availability	IoT services are ready when needed and perform acceptably.
	Elevation of privilege	Authorization	IoT users are explicitly allowed or denied access to resources.

Privacy threat analysis

TABLE 30 – LINDDUN PRIVACY THREATS

	Threat	Property		Property description
IoT systems privacy objectives expressed as threats to counter	Linkability	Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information associated with IoT entities or IoT users.
	Identifiability		Anonymity	Hiding the link between an IoT user or an IoT entity identity and an action or a piece of information
	Non-repudiation		Plausible deniability	Ability for an IoT end user or and IoT entity to deny having performed an action that other parties can neither confirm nor contradict
	Detectability		Undetectability and unobservability	Hiding the activities of an IoT user ir and IoT entity.
	Disclosure of information	Security	Confidentiality	Ability of the IoT system to hide the data content or to control the release of data content
	Unawareness	Soft Privacy	Content awareness	IoT user's consciousness regarding his own data
	Non-compliance		Policy and consent compliance	IoT stakeholder who is a PII controller to inform the IoT user who is a PII principal on the IoT system's privacy policy, or allow the IoT user to specify consents in compliance with legislation

Risk models

Risk models are used to allow for the evaluation of risks⁴³. 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 used⁴⁴:

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

Risk map

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.

⁴³ NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012

⁴⁴ 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.

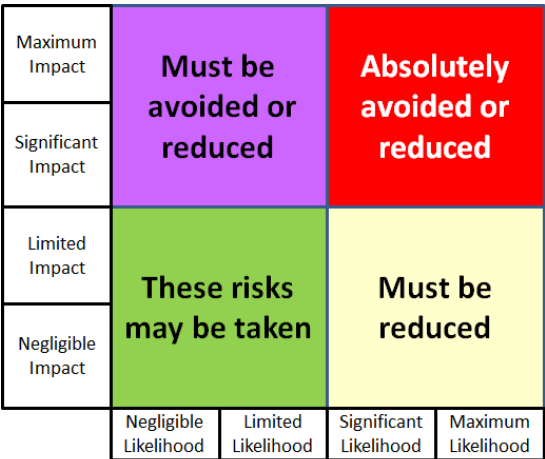


FIGURE 12 RISK MAP

Examples of Breach Impact

The table lists examples of impact on user’s privacy and on an organisation⁴⁵.

TABLE 31 - IMPACT EXAMPLES

Impact on user’s privacy	<ul style="list-style-type: none"> • loss of autonomy • exclusion • loss of liberty • physical harm • stigmatization • power imbalance • loss of trust • economic loss
Impact on the operations and business of an organisation	<ul style="list-style-type: none"> • 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.

Control categories

Table 32 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), 27701 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines), 29151 (Code of practice for personally identifiable information protection).

⁴⁵ 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

TABLE 32 – 27002 CONTROL CATEGORIES

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 33 – DATA CONTROLLER PRIVACY CONTROLS

Category	Control
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Joint PII controller
	Records related to processing PII
Obligations to PII principals	Determining and fulfilling obligations to PII principals
	Determining information for PII principals

	Providing information for PII principals
	Provide mechanism to modify or withdraw consent
	Provide mechanism to object to PII processing
	Access, correction or erasure
	PII controllers' obligations to inform third parties
	Providing copy of PII processed
	Handling requests
	Automated decision making
Privacy-by-design and by-default	Limit collection
	Limit processing
	Accuracy and quality
	PII minimization objectives
	PII de-identification and deletion at the end of processing
	Temporary files
	Retention
	Disposal
PII sharing, transfer and disclosure	PII transmission controls
	Identify basis for PII transfer between jurisdictions
	Countries and international organisations to which PII can be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties

TABLE 34 – DATA PROCESSOR PRIVACY CONTROLS

Category	Control
Conditions for collection and processing	Cooperation agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	Customer obligations
	Records related to processing PII
Obligations to PII principals	Obligations to PII principals
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfer of PII between jurisdictions
	Countries and international organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

TABLE 35 – PIMS-SPECIFIC CONTROL OBJECTIVES AND CONTROLS

Conditions for collection and processing	
Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.
Identify Lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals

Obtain and record consent	The organization shall obtain and record consent from PII principals according to the documented processes.
Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.
Contracts with PII processors	The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.
Joint PII controller	The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.
Records related to processing PII	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.
Obligations to PII principals	
Determining and fulfilling obligations to PII principals	The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.
Determining information for PII principals	The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.
Providing information to PII principals	The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.
Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.
Providing mechanism to object to PII processing	The organization shall provide a mechanism for PII principals to object to the processing of their PII.
Access, correction and/or erasure	The organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.
PII controllers obligations to inform third parties	The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.
Providing copy of PII processed	The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal.
Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.
Automated decision making	The organization shall identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.
Privacy by design and privacy by default	
Limit collection	The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.
Limit processing	The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.
Accuracy and quality	The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.
PII minimization objectives	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.
PII de-identification and deletion at the end of processing	The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).
Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.

Retention	The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.
Disposal	The organization shall have documented policies, procedures and/or mechanisms for the disposal of PII.
PII transmission controls	The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
PII sharing, transfer and disclosure	
Identify basis for PII transfer between jurisdictions	The organization shall identify and document the relevant basis for transfers of PII between jurisdictions.
Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
Records of transfer of PII	The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.
Records of PII disclosure to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

Annex V. QUESTIONNAIRE TEMPLATES ANSWERED BY THE PILOTS

iCity - Volkerwessels - Dutch Pilot



InterConnect H2020 Project WP2.3 Cybersecurity and Privacy

NAME:
Wouter Beelen
COMPANY:
VolkerWessels iCity
Contact details (e-mail):
wbeelen@volkerwessels.com

Use case Summary:
<div>Provisionally case description and related input:</div> <div>User lives in a smart /IoT apartment in the Netherlands. The user is able via an GUI (app/website) to turn on/off and control which services are active in his/her home to his preferences. Per service it becomes clear which data is collected/shared to which goal. If the users wants to know his/her actual energy consumption, then the smart meter needs to be read out to able to visualize actual energy consumption. Or when the user want to have energy optimization service active, then also relevant data from the appliances of the user needs to be shared to be able to control/optimize the use these appliances.</div>

Which organization are participating in the use case? Which responsibility does each have about the data treatment?

Operators of Essential Services:
<div>User/resident: Control over his/her data an how/when to share</div> <div>Building owner: having the connection to (individual) users/tenants for contractual purposes. Collection of building system information and based on AI (see below) predictive maintenance</div> <div>Smart solution (hardware) provider: collecting data from in house hardware/appliances to edge devices</div> <div>Cloud service provider: Secure data cloud storage / remote access of data for users and/or service provider</div>

Service provider: needing to have data to provide services (based on approval of user)

Others organizations:

University/Research: (anonymized) data for AI on datasets ie. to predict system failures or optimize systems. Or (based on consents/agreement from resident) to do profiling to make the home systems more self learning/comfortable.

What are the cyber security and privacy experiences of the pilot participants?

Cybersecurity and privacy experiences:

- DPIA:
 - Setup and management of (D)PIA process for smart District Strijp-S.
 - Setup and DPA for smart city solution providers
 - Setup of DPIA for 14 smart home apartments
- Security Risk Analysis:
 - Availability, integrity and confidentiality (in Dutch: BIV) matrix approach for Smart homes project.
 - Usage of corporate (VolkerWessels) information security policy
- Privacy by design:
 - Setup/design for smart homes project
 - Data agreement process and documents with end users
- Security by design:
 - Setup/design for smart homes project

Is there's any cybersecurity or privacy measure already in place in the pilot which could be related to the project?

Already in place processes for cybersecurity:

Corporate (VolkerWessels) information security policy
BIV matrix/approach from building owner

Already in place processes for privacy:

Corporate privacy policy with amongst others taskforce/data portal
ISO27001 from VolkerWessels Telecom (third linked partner)

Are there any cybersecurity or privacy measures planned for the pilot development?

Planned measures for cybersecurity:

Integrity checks (and as a result) upgrade, validate smart city data hub

Data security definition and checks for in-house (edge) gateways

Planned measures for privacy:
Privacy by design for pilot locations based on use cases/experiences and demands from building owners

GridNet - Greek Pilot



InterConnect H2020 Project WP2.3 Cybersecurity and Privacy

NAME:
Donatos Stavropoulos
COMPANY:
GRIDNET
Contact details (e-mail):
ds@gridnet.gr

Use case Summary:
<p>Implementation of advanced Demand Response scenarios in Residential setups.</p> <ul style="list-style-type: none"> • Application of DR on a large community of residential users (>1000). • Experiment with users interacting with the electricity and wider energy system, under real-life conditions; initially in two living lab setups and later in a large-scale setup (three different trial sites). • Validation of user acceptance and understanding of consumer behavior through mobile apps for actively engaging end-users through incentives (energy cost, social responsibility, etc.) provisioning. • Demonstrate viable concepts that ensure privacy, liability, security and trust in the resulting DR platform, by exposing only anonymized and aggregated data out of user premises.

Which organization are participating in the use case? Which responsibility does each have about the data treatment?

Operators of Essential Services:

HERON - Electricity generator – Supplier (Provide anonymized energy data out of user premises)
COSMOTE - Telecom operator - Technology Provider (Provide anonymized energy data out of user premises)
GRIDNET - Technology Provider (Provide anonymized energy data out of user premises)
WINGS - ICT supplier (Process anonymized energy data for data analytics purposes)
AUEB - Academic Institution (Interact with users through a mobile App providing incentives for engagement)

Others organizations:
GFI – DR Platform

What are the cyber security and privacy experiences of the pilot participants?

Cybersecurity and privacy experiences:
<ul style="list-style-type: none"> • DPIA: • Security Risk Analysis: • Privacy by design: Pilot partners have already incorporated in the Pilot Architecture the requirements for data/user privacy. • Biometric authentication • Notifications and alerts after specific procedures e.g. after turning on/off a device • Data minimization: Only the most necessary data of users are obtained, circulated/stored

Is there’s any cybersecurity or privacy measure already in place in the pilot which could be related to the project?

Already in place processes for cybersecurity:
<ul style="list-style-type: none"> • E2E Data Encryption from sensors/devices to backend system including: <ul style="list-style-type: none"> ○ SSL/TLS Certificates for sensors-to-MQTT Broker communication ○ VPN Tunnel for Energy Metering Gateway-to-backend communication ○ SSL/TLS Certificates for communication between the various backend components ○ Sensitive data stored in encrypted BSD server storage instances (FreeNAS Servers) ○ Remote log collection and backup via NMS solution • Security by design: <ul style="list-style-type: none"> ○ Store sensitive data in secure memory/storage

- | |
|--|
| <ul style="list-style-type: none"> ○ Do not allow clear text password storage ○ Use of standardized data formats ○ Data minimization: Only the most necessary data of users are obtained, circulated/stored |
|--|

- | |
|--|
| Already in place processes for privacy: |
| <ul style="list-style-type: none"> • Anonymized energy data (User details are not communicated) |

Are there any cybersecurity or privacy measures planned for the pilot development?

- | |
|--|
| Planned measures for cybersecurity: |
| <ul style="list-style-type: none"> • Deprecation of password logins • Public-private key server login architecture • Fine-tuning of UFW firewall rules • Hardening of LAN/VLANs isolation • Two factor authentication under consideration • Biometric authentication under consideration |

- | |
|--|
| Planned measures for privacy: |
| <ul style="list-style-type: none"> • Encryption for user sensitive data |

French Pilot



InterConnect H2020 Project WP2.3 Cybersecurity and Privacy

NAME:
COMPANY:
<i>Engie, Yncrea</i>
Contact details (e-mail):

Use case Summary:
Use cases are still under discussion and are not yet defined.

It is foreseen flexibility coming from consumer applications. Flexibility from DSO may not be part of the pilot use case

Which organization are participating in the use case? Which responsibility does each have about the data treatment?

Operators of Essential Services:
Power plant production (may not be relevant within the project)

Others organizations:
Engie <ul style="list-style-type: none"> Subcontractors and link third parties Legal constraints for power plant data Enedis

What are the cyber security and privacy experiences of the pilot participants?

Cybersecurity and privacy experiences:
<ul style="list-style-type: none"> DPIA: <ul style="list-style-type: none"> Yncrea has already done DPIA Engie’s processes need to be verified Security Risk Analysis: <ul style="list-style-type: none"> Need to follow ISO/IEC (27006) Privacy by design: <ul style="list-style-type: none"> Need to be discussed with the DPO Security by design: <ul style="list-style-type: none"> ETSI TS 103 645 Engie: Need to be validated

Is there’s any cybersecurity or privacy measure already in place in the pilot which could be related to the project?

Already in place processes for cybersecurity:
<ul style="list-style-type: none"> Engie: competence center specialised in the cloud with carry verifications, contract with Amazon <ul style="list-style-type: none"> Configuration documentation

Already in place processes for privacy:

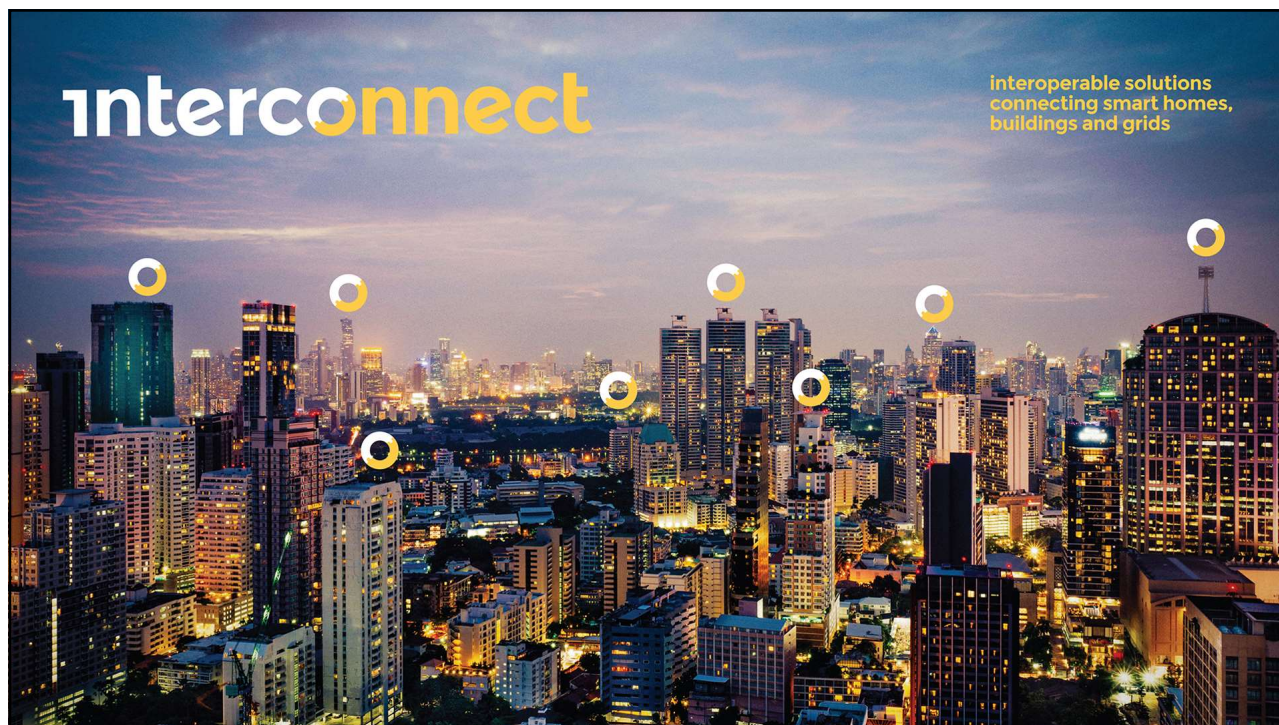
- | |
|---|
| <ul style="list-style-type: none">• DPO needs to be consulted |
|---|

Are there any cybersecurity or privacy measures planned for the pilot development?

Planned measures for cybersecurity:
To be answered after the use cases definition

Planned measures for privacy:
A DPIA seems essential

Annex VI. SLIDES OF WEBINAR ON THE CONCEPT OF SECURITY AND PRIVACY PLAN – NOVEMBER 3RD 2020



1



Webinar : concept of security and privacy plan

WP5 – Digital platforms and marketplace

T5.3 Applying practice for security and privacy policy compliance

Speaker – Antonio Kung, TRIALOG

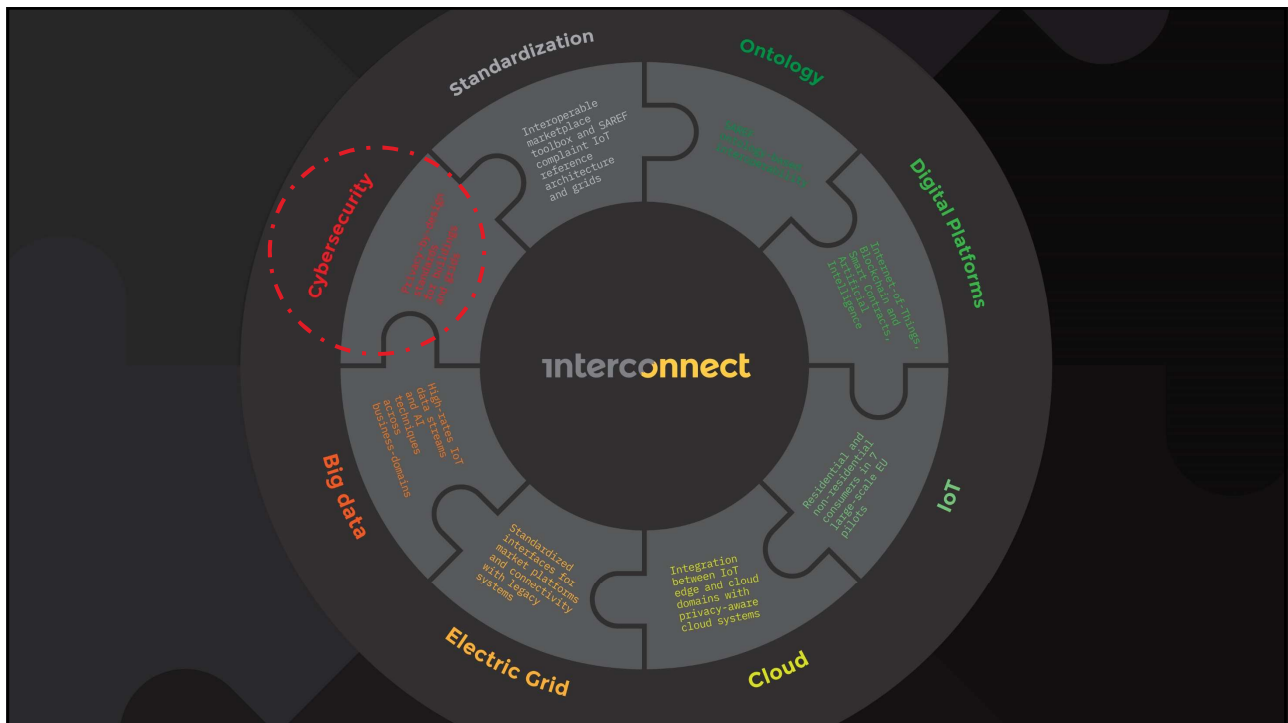
Supporting experts: Estibaliz Arzoz Fernández, Amélie Gyrard, Yannick Huc

Date: November 3rd, 2020

2

interconnect

2



3

Outline of webinar



- **Introduction (15mn)**
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- **Implementation guidelines (20mn)**
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- **Walkthrough (25mn)**
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- **Next steps (5mn)**
- **Q&A (10mn)**

4

interconnect

4

Outline of webinar



■ Introduction (15mn)

- Speaker
- Recap on Interconnect work and objectives
- Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan

■ Implementation guidelines (20mn)

- SPOCS
- Methodology
- Content of plan
- Landscape of standardization work on security and privacy

■ Walkthrough (25mn)

- Policy framework
- Security and privacy plan template
- Security and privacy risk analysis support

■ Next steps (5mn)

■ Q&A (10mn)

5

interconnect

5

Speaker Introduction



■ CEO - Trialog



- Integration of technology innovation in cyber physical systems
 - CPL technology for smart meters (G3-PLC)
 - Charging technology (ISO 15118, Chademo)
 - Cooperative ITS technology
- Cross-cutting concerns and technology
 - Cybersecurity and privacy, IoT, Data spaces and AI

■ Speaker – CPS engineering background

- Standardisation
 - ISO/IEC
 - SC27 (cybersecurity and privacy)
 - SC41 (IoT)
 - AG8 (meta reference architecture)
 - ISO
 - PC317 (privacy-by-design for consumer goods and services)
 - AIOTI liaisons officer to ISO/IEC SC41
- Research & Innovation projects
 - PRIPARE, AUTOMAT, ACCRA, Create-IoT, PDP4E, Interconnect

6

interconnect

6

Outline of webinar



- Introduction (15mn)
 - Speaker
 - **Recap on Interconnect work and objectives**
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

7

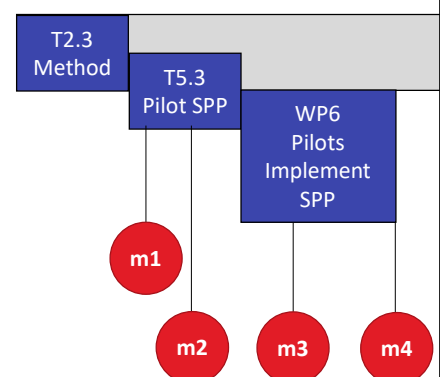
interconnect

7

Interconnect work on security and privacy



- Activities
 - Method to create a security and privacy plan (SPP)
 - T2.3 M1-Oct 2019, M36-Sept 2022
 - Pilots use methods to define their SPP
 - T5.3 M12-Oct 2020, M18-Mars 2021
 - Pilots implements SPP and provide feedback
 - WP6 M3-Nov 2020, M48-Sept 2023
- Meetings with pilot
 - Explain method
 - Meeting 1: Nov 3, 2020 - webinar
 - Training on SPP building
 - Meeting 2: before March 21 - individual pilot meeting
 - Apply security and privacy analysis
 - Meeting 3: individual pilot meeting
 - Collect return from experience
 - Meeting 4: M36-sept 2022 - Common workshop



Innovations:

- Ecosystem plan
- Combining security and privacy

8

interconnect

8

Results from security and privacy practice

- D2.2 Privacy and security design principles and implementation guidelines
 - Dec 2020
- D5.3 Security, Cyber-security and privacy protection action plan and results
 - Mar 2021
- Material for impact including policy framework analysis
 - Sept 2022

The diagram illustrates the flow from D2.2 to D5.3 and finally to Impact material on innovations. A timeline below shows the progression of tasks: T2.3 Method, T5.3 Pilot SPP, and WP6 Pilots Implement SPP. Milestones m1, m2, m3, and m4 are marked along the timeline.

9

interconnect

9

The timeline diagram for T5.3 Applying practice for security and privacy policy compliance shows the following key events and deliverables:

- Oct'20:** Planning (M12)
- Nov'20:** Meeting 1 (webinar)
- Dec'20:** Meeting 2 (all pilots) + Meeting 3 (some pilots)
- Jan'21:** D2.2 (Submission)
- Feb'21:** D5.3 (Draft)
- Mar'21:** Reports (M18), D5.3 (submission)

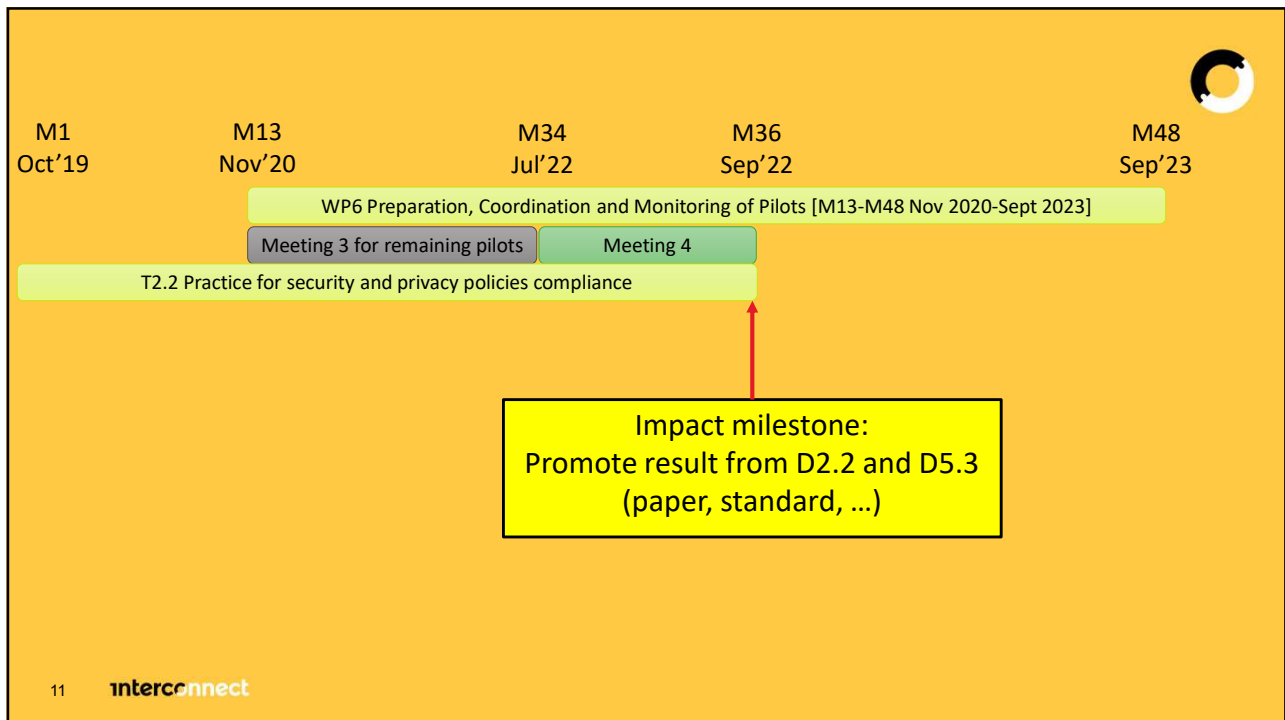
Internal milestones include: Finalisation of D2.2.

T5.3 Applying practice for security and privacy policy compliance

10

interconnect

10



11

The slide has a white background and a circular logo with a black and white swirl in the top right corner. The title 'Outline of webinar' is in bold black text. Below the title is a list of topics, each preceded by a blue square bullet point. The first topic is 'Introduction (15mn)' with sub-bullets 'Speaker', 'Recap on Interconnect work and objectives', and 'Security and privacy principles in Interconnect' (the latter is highlighted with a yellow background). The second topic is 'Implementation guidelines (20mn)' with sub-bullets 'SPOCS', 'Methodology', 'Content of plan', and 'Landscape of standardization work on security and privacy'. The third topic is 'Walkthrough (25mn)' with sub-bullets 'Policy framework', 'Security and privacy plan template', and 'Security and privacy risk analysis support'. The fourth topic is 'Next steps (5mn)' and the fifth is 'Q&A (10mn)'. In the bottom left corner, the number '12' and the 'interconnect' logo are visible.

12

Promise and Challenge for future energy/flexibility ecosystems

Digitalisation

A Venn diagram with three overlapping circles labeled IoT, AI, and Digital twin.

Promise

A Venn diagram with three overlapping circles labeled Smart Energy, Domain Y, and Domain X.

Flexibility of energy offer

Challenge

A Venn diagram with three overlapping circles labeled Trustworthiness, Ecosystems, and Systems of systems.

Complex systems

13 interconnect

13

Example of Challenge: Privacy in Smart City Ecosystems

A flowchart illustrating the privacy process in smart city ecosystems. It shows interactions between a Municipality stakeholder, Citizen, Data Controller, Data processor, Integrator, and Supplier. Key steps include Requests, Give consent, Express preference, Agree, Comply, and Apply, leading to Privacy Obligations, PIA and PbD Purpose known, and Requirements Purpose unknown.

14 interconnect

14

Security and privacy principles



■ Principle 1: policy framework analysis

- Policy framework analysis to be provided by each pilot
 - Trust analysis
 - Engagement analysis
 - Security and privacy engineering
- Analysis will be provided by the pilots when enough experience has been gained in a specific workshop (meeting 4)

Two viewpoints

- The pilot viewpoint
- The future pilot ecosystem viewpoint

15 interconnect

15

Security and privacy principles



■ Principle 2: security and privacy plan

- A security and privacy plan will be specified by each pilot:
 - Common process
 - Content of the plan based on ISO/IEC 27570, ecosystem privacy plan, extended to include security.
 - governance management plan
 - data management plan
 - risk management plan
 - engineering management plan
 - citizen engagement plan
- individual pilot workshop (meeting 2 and 3)
 - How to use security and privacy plan template
 - Work on security and privacy risk analysis

Two viewpoints

- The pilot viewpoint
- The future pilot ecosystem viewpoint

16 interconnect

16

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

17

interconnect

17

Methodology to create a security and privacy plan



- Process
 - SPOCS (Security and Privacy Policy Compliance Solution)
- Outcome
 - SPP (Security and Privacy plan)

18

interconnect

18

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

19

interconnect

19

Governance management plan



Rules, legislations, applicable international standards
Governance body
Organizations, organizations structures and responsibility
Rules and procedure
Continual improvement

- Two viewpoints
- The pilot viewpoint
 - The future pilot ecosystem viewpoint

20

interconnect

20

Data management plan



Ownership and PII stakeholders
Data management agreements
Data description
Data exchanges
Data access monitoring

- Two viewpoints
- The pilot viewpoint
 - The future pilot ecosystem viewpoint

21

interconnect

21

Risk management plan



Risk analysis needs
Risk analysis methodology
Risk analysis schedule

- Two viewpoints
- The pilot viewpoint
 - The future pilot ecosystem viewpoint

22

interconnect

22

Engineering management plan



Engineering needs
Engineering process
Engineering schedule

- Two viewpoints
- The pilot viewpoint
 - The future pilot ecosystem viewpoint

23

interconnect

23

Citizen engagement plan



Citizen engagement needs
Citizen engagement process
Citizen engagement schedule

- Two viewpoints
- The pilot viewpoint
 - The future pilot ecosystem viewpoint

24

interconnect

24

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

25

interconnect

25

Landscape of standardisation work on security and privacy



- Cybersecurity
 - Risk
 - ISO/IEC 27005 Information security risk management
 - Information systems
 - ISO/IEC 27001 ISMS requirements
 - ISO/IEC 27002 Information security controls
 - Lifecycle and ecosystems
 - NIST cybersecurity framework
 - ISO/IEC 27101 Cybersecurity framework development guidelines

26

interconnect

26

Landscape of standardisation work on security and privacy



■ Privacy

- Risk
 - ISO/IEC 29134 Guidelines for privacy impact assessment
 - NISTIR 8062 Introduction to privacy engineering and risk management in federal systems
- Information systems
 - ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
 - Microsoft data protection / privacy mapping project
- Lifecycle and ecosystem
 - NIST Privacy framework
 - ISO/IEC 27570 Privacy guidelines for smart cities
 - ISO/IEC 27556 User-centric framework for the handling of PII based on privacy preferences
- Engineering
 - ISO/IEC 27550 - Privacy engineering for system life cycle processes
 - ISO/IEC 31700 Privacy-by-design for consumer goods and services
 - New ISO standard — Privacy operationalisation model and method for engineering (POMME)

27 interconnect

27

Landscape of standardisation work on security and privacy



■ IoT security and privacy

- ISO/IEC 27400 Security and privacy guidelines for IoT
- ISO/IEC 27402 – IoT security and privacy – device baseline requirements
- ISO/IEC 27403 IoT security and privacy – guidelines for IoT domotics
- NISTIR 8200 Interagency report on the status of international cybersecurity standardization for the Internet of Things

■ Domains

- IEC 63443 series
- NIST 7628 guidelines for smart grid cyber-security

28 interconnect

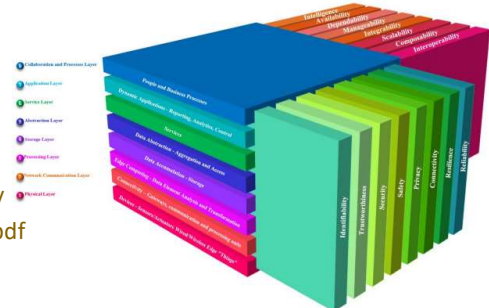
28

Landscape of standardisation work on security and privacy



■ Architecture

- ISO/IEC 30141 IoT reference architecture
- AIOTI reference architecture
- Create-IoT 3-D architecture
 - https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf



■ Trustworthiness

- ISO/IEC 30141 IoT reference architecture
 - Trustworthiness view
- ISO/IEC 30149 IoT trustworthiness principles
- ISO/IEC 30147 Integration of trustworthiness in IoT lifecycle processes
- Study on trustworthiness reference architecture

29 interconnect

29

Outline of webinar



■ Introduction (15mn)

- Speaker
- Recap on Interconnect work and objectives
- Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan

■ Implementation guidelines (20mn)

- SPOCS
- Methodology
- Content of plan
- Landscape of standardization work on security and privacy

■ Walkthrough (25mn)

- Policy framework
- Security and privacy plan template
- Security and privacy risk analysis support

■ Next steps (5mn)

■ Q&A (10mn)

30 interconnect

30

IoT policy framework



Trust analysis template	
Socio-economical perspective	To be provided by pilot
Business perspective	To be provided by pilot
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	To be provided by pilot

Engagement analysis template	
Engagement on ethics	To be provided by pilot
Engagement on standards	To be provided by pilot
Engagement on legislation	To be provided by pilot
Engagement on contracts	To be provided by pilot

Security and privacy analysis template	
Risk management (use the Automat security and privacy risk analysis template)	To be provided by pilot
Designing security and privacy:	To be provided by pilot
Assuring security and privacy	To be provided by pilot

31 interconnect

31

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

32 interconnect

32

Walkthrough template

1	Security and Privacy Plan Context
Application Name	
Summary	
Description	

2	Governance Management Plan
Rules and legislation	
International Standards	
2.1	Governance Body
Information Security Manager	
Data Protection Officer	
Other roles	
2.2	Organisation responsibility
Entity 1	Entity Name
	Role
	Address
	Contact(s)
	Entity Type
Structure of responsibility	
2.3	Rules and procedure
Meetings	
Nomination	
Publication of minutes	
2.4	Continual improvement
Meetings	
Evaluation procedure	

33

33

3	Data Management Plan
3.1	Pilot needs and resources for security and privacy data management
Ownership of data	
PII Controller	
PII Processors	
PII Principals	
3.2	Data Management Process
3.2.1	Agreements
Agreement approach	
Agreement 1	Organizations
	Agreement template
3.2.2	Data description
Data 1	Identification of data
	Type of data
	Life Cycle
	Data description
3.2.3	Data exchange
Data flow	
Data access control chart	
3.2.4	Data access monitoring
Data access verification procedure	

Walkthrough template

4	Risk Management Plan
4.1	Pilot needs and resources for security and privacy risk management
Context for privacy analysis	
Context for security analysis	
4.2	Risk management process
4.2.1	Security
Methodology	
Schedule	
Template	
4.2.2	Privacy
Methodology	
Schedule	
Template	

5	Engineering Management Plan
Pilot needs and resources for security and privacy engineering	
Engineering process	
Schedule	

6	Citizen Engagement Plan
Pilot needs and resources for engagement	
Engagement process	
Schedule	

34

34

17

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

35 interconnect

35

Security threat analysis



	Threat	Property	Property description
IoT systems security objectives expressed as threats to counter	Spoofing	Authentication	The identity of IoT entities or IoT users is established (or you are willing to accept anonymous entities).
	Tampering	Integrity	IoT data and system resources are only changed in appropriate ways by appropriate people.
	Repudiation	Nonrepudiation	IoT users cannot perform an action and later deny performing it.
	Information disclosure	Confidentiality	Data is only available to the IoT users intended to access it.
	Denial of Service	Availability	IoT services are ready when needed and perform acceptably.
	Elevation of privilege	Authorization	IoT users are explicitly allowed or denied access to resources.

36 interconnect

36

Privacy threat analysis



	Threat	Property	Property description
IoT systems privacy objectives expressed as threats to counter	Linkability	Hard privacy	Unlinkability Hiding the link between two or more actions, identities, and pieces of information associated with IoT entities or IoT users.
	Identifiability		Anonymity Hiding the link between an IoT user or an IoT entity identity and an action or a piece of information
	Non-repudiation		Plausible deniability Ability for an IoT end user or and IoT entity to deny having performed an action that other parties can neither confirm nor contradict
	Detectability		Undetectability and unobservability Hiding the activities of an IoT user ir and IoT entity.
	Disclosure of information	Security	Confidentiality Ability of the IoT system to hide the data content or to control the release of data content
	Unawareness	Soft Privacy	Content awareness IoT user's consciousness regarding his own data
	Non-compliance		Policy and consent compliance IoT stakeholder who is a PII controller to inform the IoT user who is a PII principal on the IoT system's privacy policy, or allow the IoT user to specify consents in compliance with legislation

37 interconnect

37

Risk models



$$\text{Security and Privacy risk level} = \text{Likelihood of breach} \times \text{Impact of breach}$$

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

38 interconnect

38

Impact examples (privacy – see ISO/IEC 27550)



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

39 interconnect

39

Privacy engineering design strategies



Design strategy		Description	Privacy control examples
Data oriented strategies	Minimize	Limit as much as possible the processing of PII	Selection before collection Anonymization
	Separate	Distribute or isolate personal data as much as possible, to prevent correlation	Logical or physical separation Peer-to-peer arrangement Endpoint processing
	Abstract	Limit as much as possible the detail in which personal data is processed, while still being useful	Aggregation over time (used in smart grids) Dynamic location granularity (used in location-based services) k-anonymity
	Hide	Prevent PII from becoming public or known.	Encryption Mixing Perturbation (e.g. differential privacy, statistical disclosure control) Unlinking (e.g. through pseudonymization) Attribute based credentials
Process oriented strategies	Inform	Inform PII principals about the processing of PII	Privacy icons Layered privacy policies Data breach notification
	Control	Provide PII principals control over the processing of their PII.	Privacy dashboard Consent (including withdrawal)
	Enforce	Commit to PII processing in a privacy friendly way, and enforce this	Sticky policies and privacy rights management Privacy management system Commitment of resources Assignment of responsibilities
	Demonstrate	Demonstrate that PII is processed in a privacy friendly way.	Logging and auditing Privacy impact assessment Design decisions documentation

40 interconnect

40

27002 Controls	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

41

Data controller Privacy controls	Category	Control
	Conditions for collection and processing	Identify and document purpose
		Identify lawful basis
		Determine when and how consent is to be obtained
		Obtain and record consent
		Privacy impact assessment
		Contracts with PII processors
	Obligations to PII principals	Joint PII controller
		Records related to processing PII
		Determining and fulfilling obligations to PII principals
		Determining information for PII principals
		Providing information to PII principals
		Provide mechanism to modify or withdraw consent
		Provide mechanism to object to PII processing
		Access, correction or erasure
		PII controllers' obligations to inform third parties
		Correction or erasure
	Privacy-by-design and by-default	Providing copy of PII processed
		Handling requests
		Automated decision making
		Limit collection
		Limit processing
		Accuracy and quality
		PII minimization objectives
		PII de-identification and deletion at the end of processing
	PII sharing, transfer and disclosure	Temporary files
		Retention
		Disposal
		PII transmission controls
		Identify basis for PII transfer between jurisdictions
		Countries and international organisations to which PII might be transferred
		Records of transfer of PII
		Records of PII disclosure to third parties

42

Data processor privacy controls



Category	Control
Conditions for collection and processing	Cooperation agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	Customer obligations
Obligations to PII principals	Records related to processing PII
	Obligations to PII principals
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfer of PII between jurisdictions
	Countries and international organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

43 interconnect

43

Outline of webinar



- Introduction (10mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (25mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

44 interconnect

44

Meeting 2 (security and privacy plan creation)



- One meeting per pilot - Dec 2020 – Feb 2021
- Objective: create a security and privacy plan
- Uses the security and privacy plan template defined in D2.2 Annex III
- Format
 - Session 1 – 3 hours
 - Security and privacy plan context
 - Governance management plan
 - Data management plan
 - Session 2 – 3 hours
 - Risk management plan
 - Engineering management plan
 - Citizen engagement plan

45

interconnect

45

Meeting 3 (security and privacy risk analysis)



- One meeting per pilot - Feb 2020 – July 2021
- Objective: carry out a security and privacy analysis
 - Identification of threats
 - Evaluation of impact
 - Identification of risk treatments
- Uses the security and privacy risk analysis support in D2.2 Annex IV
- Format
 - Session 1 – 3 hours
 - Specification of systems to protect
 - Identification of risks
 - Session 2 – 3 hours
 - Evaluation of impact
 - Identification of treatments (controls)
 - Assessment

46

interconnect

46

Meeting 4 (policy framework analysis)



- One meeting for all pilot - Sept 2022
- Pilots to provide a debriefing on their feedback on policy framework
 - Trust analysis
 - Engagement analysis
 - Security and privacy analysis
- Uses the policy framework template defined in D2.2 Annex II
 - For an example of policy framework analysis see Create-IoT deliverable
 - https://european-iot-pilots.eu/wp-content/uploads/2020/06/D05_02_WP05_H2020_CREATE-IoT_Final.pdf

47

interconnect

47

How meetings 2, 3, 4 will work



- Work prior to meeting
 - Material provided by Trialog to pilot prior to meeting
 - Pilot prepare preliminary analysis
- Meeting
 - Presentation of meeting result by Pilot stakeholder
- Work further to meeting
 - Summary prepared by Trialog
 - Summary reviewed by pilot

48

interconnect

48

Outline of webinar



- Introduction (15mn)
 - Speaker
 - Recap on Interconnect work and objectives
 - Security and privacy principles in Interconnect
 - Policy framework analysis
 - Security and privacy plan
- Implementation guidelines (20mn)
 - SPOCS
 - Methodology
 - Content of plan
 - Landscape of standardization work on security and privacy
- Walkthrough (25mn)
 - Policy framework
 - Security and privacy plan template
 - Security and privacy risk analysis support
- Next steps (5mn)
- Q&A (10mn)

49

interconnect

49

interconnect

interoperable solutions
connecting smart homes,
buildings and grids

FINANCING



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

PROJECT CONTACT

interconnect_project@inesctec.pt

DURATION

01.10.2019 / 30.09.2023

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.

50