H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.02

IoT Policy Framework Evaluation and Final IoT Policy Framework

Revision: 1.00
Due date: 31-12-2019 (m36)
Actual submission date: 20-01-2020
Lead partner: TL

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D05.02 IoT Policy Framework Evaluation and Final IoT Policy Framework**				
Status	Final	**Due**	m36	**Date**	31-12-2019
Author(s)	Antonio Kung (TL), Ovidiu Vermesan (SINTEF), Ross Little Armitt (ATOS), Dimitra Stefanatou (AL), Prakrii Pathania (A), Sebastien Ziegler (MI), Pasquale Annicchino (AS). This deliverable benefitted from the kind participation of the large-scale pilot projects: • ACTIVAGE: Sofia Segkouli (Information Technologies Institute, Center for Research and Technology, Hellas) • AUTOPILOT: Ovidiu Vermesan (SINTEF) • MONICA: Trine F. Sørensen (In-Jet ApS) • IoF2020: Simone van der Burg (Wageningen University & Research) • SYNCHRONICITY: Sébastien Ziegler (MI), Pasquale Annichinno (AS)				
Editor	Antonio Kung (TL)				
DoW	The evaluation report as well as an updated IoT Policy Framework (D05.01) and a recommendation report beyond the project.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	26-01-2019	SINTEF	Template.
0.01	26-11-2019	SINTEF	Initial version.
0.02	23-10-2019	TL	ToC/structure.
0.03	22-12-2019	TL	Input for standardisation, ACTIVAGE and AUTOPILOT.
0.04	23-12-2019	SINTEF	Input AUTOPILOT.
0.05	03-01-2020	SINTEF	Overall updates.
0.06	05-01-2020	AS, TL	Input SYNCHRONICITY, Analysis of LSPs projects feedback.
0.07	07-01-2020	MI	Input SYNCHRONICITY and Standardisation.
0.08	11-01-2020	ATOS, TL	Analysis of IoF2020 and conclusions.
0.09	13-01-2020	TL, ATOS, AL	Summary, Further input onIoF2020, review of whole deliverable.
1.00	17-01-2020	SINTEF	Final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Publishable Summary

Deliverable D05.02 focuses on the evaluation of the work carried out on an IoT policy framework in the frame of the IoT large scale pilot program. An initial specification of the IoT policy framework (D05.01) was made available in 2017 to the ACTIVAGE, AUTOPILOT, IoT2020, MONICA, and SYNCHRONICITY projects. The evaluation takes into account standardisation as well as the viewpoint of each pilot. The deliverable will be useful to further pilots, the research community and a larger audience including industry, public administration and standardization bodies. The deliverable first provides a landscape on standardisation focusing on the wealth of on-going work in ISO, IEC and ITU-T. It then covers the three pillars of an IoT policy framework:

- Trust, which includes a socio-economic perspective, a business perspective, and a technical perspective;
- Organization engagement which includes ethics, standards, legislation and contracts; and
- Security and privacy engineering includes risk management, design of security and privacy, and assurance of security and privacy.

For each of the three pillars, an analysis of the standardisation landscape, and inputs from large scale pilots are analysed. The result is collected into several policy recommendations:

- Concerning trust, (1) enable economic progress associated with social progress, (2) integrate factors relevant for trust considering user's perception and the social environment, and (3) leverage an agreed architecture description and terminology;
- Concerning organisation engagement, (1) practice for business ethics and corporate social responsibility, (2) foster the contribution and adoption of standards related to trust (assessment, measures, assurance), (3) monitor the evolution of legislation related to IoT on security and privacy, and (4) focus on supply chain contractual practice; and
- Concerning security and privacy engineering, (1) research and innovation projects should gain knowledge on risk management of IoT systems (architecture considerations, exchanging risk information in an ecosystem and use of common knowledge), (2) research and innovation projects should take an integrated X-by-design approach, including citizen engagement and user-centred process, (3) research and innovation projects should gain knowledge on assurance of security and privacy in IoT.

1.2 Non-publishable Information

The document is public.

2. INTRODUCTION

2.1 Purpose of deliverable

This deliverable extends a first deliverable D05.01 IoT Policy Framework, published in September 2017. Its purpose is the following:

The IoT Policy Framework presents a conceptual structure that aims to organise and clarify the collective principles, functions, definitions, requirements and practices, created through the technical expertise of stakeholders within the IoT European Large-Scale Pilots Programme stakeholders through a process and organised methodology within this active stakeholder community.

2.2 Target group

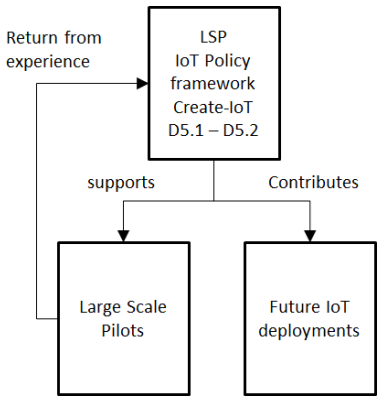


Figure 1: Target group for the IoT policy framework.

Figure 1 shows the target group of the IoT policy framework:

- The large-scale pilots stakeholders. D05.01 and D05.02 provide an IoT policy framework which can be used to support future large-scale projects,
- Future IoT deployments. D05.01 and D05.02 can be used as an input to a IoT policy framework that will be used for deployment.

This target group will be involved on an event in March 2020 (IoT Policy Framework Common Event) that will be reported in deliverable D05.08.

2.3 Content of deliverable

D05.01 was made available at the very start of the IoT European Large-Scale Pilot Programme. D05.02 enriches D05.01 as follows:

- It takes include the feedback from the large-scale pilots, in particular the inputs gained within AG05 during year 2 and year 3.
- It considers the standardisation landscape, highlighting contributions made by the large-scale pilot programme itself as well as the AIOTI community.
- It exposes the experience and knowledge gathered by the first wave of large-scale pilots that can be used by further large-scale pilots.
- It provides recommendations on further challenges and contributions which the new large-scale pilots in the area of future IoT policy frameworks.

The deliverable includes:

- A section describing the large-scale pilot programme,

- A section on a return of experience on trust in an IoT policy framework,
- A section on a return of experience on engagement in an IoT policy framework,
- A section on a return of experience on security and privacy in an IoT policy framework,
- A section based on D05.01 integrating the updates from the return of experience, and
- A conclusion summarizing what has been learned, and a list of recommendations for future large-scale pilots.

2.4 Inputs used for this Deliverable

This deliverable has used extensive inputs from the large-scale pilots. The table below lists the deliverables as well as publications from them.

Table 1: Inputs used from Large Scale Pilots Deliverables

Project	Document
ACTIVAGE[1]	End-to-end Security and Privacy-by-Design for AHA-IoT Applications and Services Next Generation Internet of Things Distributed Intelligence at the Edge IERC 2018 Cluster Chapter 4
AUTOPILOT[2]	D1.9 Initial Specification of Security and Privacy for IoT-enhanced AD D5.4 IoT Policy Framework for autonomous vehicles applications
IoF2020[3]	D3.1 Guidelines for use case analysis & design D3.2 The IoF2020 use case architectures and overview of the related IoT systems D3.3 Opportunities ad barriers in the present regulatory situation for system development D3.4 Policy Recommendations D3.5 Guidelines for the use of IoT related Standards in Smart Farming and Food Security D7.1 Ethics of smart farming: Current questions and directions for responsible innovation towards the future
MONICA[4]	D9.1 Impact Assessment and Validation Framework D11.1 Collective Awareness Platform for Citizen Engagement and Co-creativity D12.5 Report on Standards, Regulations, and Policies for IoT Platforms
SYNCHRONICITY[5]	D1.3 Guidelines for SYNCHRONICITY architecture D1.4 Privacy-by-design methodology & PIA D1.10 First set of citizen-centred methods and tools D2.2 Reference Architecture for IoT Enabled Smart Cities D2.4 Basic data marketplace enablers D2.10 Reference Architecture for IoT Enabled Smart Cities D6.2 Internet of Things Standardization Report

The table below lists the many initiatives on standardisation related to IoT that have been taken into consideration in this deliverable. It is worth noting that the majority of them are still on-going, justifying the considerable work that CREATE-IoT, the large-scale pilots, AIOTI, the EC and the industry stakeholders have dedicated in being actively engaged.

Table 2: Inputs used from Standardisation Projects

Committee	Document
ITU-T FG-DPM	Framework for security, privacy, risk and governance in data processing and Management[6]

[1] http://www.activageproject.eu/communication-room/public-documents/
[2] https://autopilot-project.eu/deliverables/
[3] https://www.iof2020.eu/about/deliverables
[4] https://www.monica-project.eu/public-deliverables/
[5] https://synchronicity-iot.eu/media/

	Overview of technical enablers for trusted data[7]
ISO/JTC1 WG13	Standard in development: ISO/IEC 24462 Ontology for ICT Trustworthiness Assessment
ISO/JTC1 AG8	Report in development: Meta Reference Architecture
ISO/JTC1 SC27	Standard published in August 2019: ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines Standard published in September 2019: ISO/IEC 27550 Privacy engineering for system lifecycle processes Standard in development: ISO/IEC 24391 Guidelines for IoT-domotics security and privacy Standard in development: ISO/IEC 27030 Security and privacy guidelines for IoT Standard in development: ISO/IEC 27101 Guidelines for cybersecurity frameworks Standard in development: ISO/IEC 27570 Privacy guidelines for smart cities Standard in development: ISO/IEC 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences Report in development: Impact of AI on privacy Proposal for the development of a standard on consent record information structure Proposal for the development of a standard on organisational privacy
ISO/JTC1 SC38	Standard in development: ISO/IEC 23751 Data sharing frameworks
ISO/JTC1 SC41	Standard in development: ISO/IEC 30141 Edition 2 – IoT reference architecture Standard in development: ISO/IEC 30147 Integration of trustworthiness in ISO/IEC/IEEE 15288 System life cycle processes Standard in development: ISO/IEC 30149 IoT trustworthiness frameworks Standard in development: ISO/IEC 30165 Real-time IoT Report in development: IoT use cases
ISO/JTC1 SC42	Standard in development: ISO/IEC 23894 – AI risk management Standard in development: ISO/IEC 240278 – Bias in AI systems and AI aided decision making Standard in development: ISO/IEC 24028 – Overview of trustworthiness in artificial intelligence Standard in development: ISO/IEC 24029-1 – Assessment of robustness of neural networks
ISO TC22/SC32/WG11	Standard in development: ISO 21434 – Road vehicles cybersecurity engineering
ISO PC317	Standard in development: ISO 31700 – privacy-by-design for consumer goods and services
ISO TMBG	Standard published in 2010: ISO 26000 – guidance on social responsibility
ISO CASCO	Standard published in August 2019: ISO 17033 – Ethical claims and supporting information — Principles and requirements

2.5 Contribution Approach and Role of Partners

The method used to create this deliverable was as follows

- We summarised the IoT policy framework (in D05.01) in section 4.1 for trust, in section 5.1 for organisation engagement, and in section 6.1 for security and privacy engineering.
- We provided a survey of the work carried out on standards on the same topics in section 4.2 for trust, in section 5.2 for organisation engagement, and in section 6.2 for security and privacy engineering.
- We collected the return from experience from the pilots. Several e-meetings were organised in the activity group AG05, a template was provided covering topics described in the table below. The results were then provided in tables that have been reproduced verbatim in

[6] https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-DPM-2019-4.1-PDF-E.pdf
[7] https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-DPM-2019-4.3-PDF-E.pdf

section 4.3 for trust, section 5.3 for organisation engagement, and in section 6.3 for security and privacy engineering.
- We provided an overall analysis, in section 4.4 for trust, in section 5.4 for organisation engagement, and in section 6.4 for security and privacy engineering.
- Conclusions and recommendations were extracted from the overall analysis with a focus on the objectives of task 5.1[8]. They are reported in section 7.2.

Table 3: Topics covered in the feedback provided by large-scale pilot projects

Trust	Socio-economical perspective of trust
	Business perspective of trust
	Technical perspective of trust: components
Organisation engagement	Engagement on ethics
	Engagement on standards
	Engagement on legislation
	Engagement on contracts
Security and privacy engineering	Risk management
	Designing security and privacy
	Assuring security and privacy

The partners involved in this report are the following:

- **TL** edited the document, and contributed to the overall analysis of the IoT policy framework, to the elaboration of the standardisation landscape, based on participation to IoT standardisation aspects (architecture, security and privacy, interoperability and use cases), to the review of ACTIVAGE and MONICA large-scale project deliverables, to the identification of commonalities and to the elaboration of recommendations beyond CREATE-IoT.
- **SINTEF** contributed to the development of a European and global policy IoT framework that encourage the development of a robust and trusted IoT ecosystem that promotes critical capabilities, including embedded and distributed intelligence, connectivity, interoperability, privacy and security, intelligent analytics and smart data. The work in this document focused on aligning and integrating the AUTOPILOT IoT policy framework for autonomous vehicles applications including trust, security, privacy and stakeholders engagement that comprises a set of principles that form the basis of making rules and guidelines, and give an overall direction to planning, development and deployment of technologies and solutions for autonomous vehicles, IoT and AI systems. The proposed policies are presented at high-level are technology neutral, and concern risks being a prerequisite for the implementation-specific information, which is part of the security standards, procedures and guidelines.
- **ATOS** reviewed IoF2020 deliverables and provided input to identify the commonalities for trust framework (with TL).
- **AL** provided and update of the IoT engagement framework captured under D05.01 in line with the latest regulatory developments[9], identified the commonalities for IoT engagement framework (with TL) and reviewed the deliverable.

[8] This task aims to create an IoT policy framework to address issues of horizontal nature and common interest (i.e. privacy, end-to-end security, societal, ethical aspects and legal issues) in a coordinated and consolidated manner across the IoT activities and pilots. The work will focus on setup a trusted environment as set above. The task will provide further development and exploitation of mechanisms towards trusted, safe, secure and legal best practices and a potential label ("Trusted IoT"). In this context, issues such as IoT Life Cycle, trust definitions, common understanding, and common durable adoption reference model will be covered.

[9] Note that the latest regulatory developments pertinent to IoT are detailed under D05.06 of CREATE-IoT project, currently under review by the EC services.

- **MI** integrated input from a paper prepared by AG05[10] and standardisation work from SYNCHRONICITY.
- **AS** reviewed SYNCHRONICITY deliverables and identified commonalities for security and privacy framework (with TL).
- **BLU** reviewed the conclusions in anticipation of preparation for an AIOTI publication.

[10] Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things (being submitted for publication)

3. LARGE SCALE PILOTS OVERVIEW AND LATEST DEVELOPMENTS

3.1 Large Scale Pilots Overview

The IoT European Large-Scale Pilots Programme[11] was started in 2017 covering the following large-scale pilots (LSP):

- Smart living environments for ageing well (ACTIVAGE)
- Autonomous vehicles in a connected environment (AUTOPILOT)
- Smart Farming and Food Security (IoF2020)
- Wearables for smart ecosystems (MONICA)
- IoT solutions for smart cities (SYNCHRONICITY)

The programme projects:

- focus on IoT approaches to specific real-life industrial/societal challenges,
- involve stakeholders from the supply side and the demand side,
- contain all the technological and innovation elements, and
- include tasks related to the use, application and deployment as well as the development, testing and integration activities.

The table below provides a summary of the five large-scale pilots in the programme[11].

Table 4: Description of Large-Scale Pilots

Project	Description
ACTIVAGE	ACTIVAGE (ACTivating InnoVative IoT smart living environments for AGEing well) brings together 48 partners from 9 European countries with the objectives to build the first European IoT ecosystem across 9 Deployment Sites (DS) in seven European countries, reusing and scaling up underlying open and proprietary IoT platforms, technologies and standards, and integrating new interfaces needed to provide interoperability across these heterogeneous platforms, that will enable the deployment and operation at large scale of Active & Healthy Ageing IoT based solutions and services, supporting and extending the independent living of older adults in their living environments, and responding to real needs of caregivers, service providers and public authorities. The project delivers the ACTIVAGE IoT Ecosystem Suite (AIOTES), a set of Techniques, Tools and Methodologies for interoperability at different layers between heterogeneous IoT Platforms and an Open Framework for providing Semantic Interoperability of IoT Platforms for AHA, addressing trustworthiness, privacy, data protection and security. User-demand driven interoperable IoT-enabled Active & Healthy Ageing solutions are deployed on top of the AIOTES in every DS, enhancing and scaling up existing services, for the promotion of independent living, the mitigation of frailty, and preservation of quality of life and autonomy.
AUTOPILOT	AUTOPILOT (AUTOmated driving Progressed by Internet Of Things) brings together 43 partners from 14 European countries and 1 from South Korea with the objectives to increase safety, provide more comfort and create many new business opportunities for mobility services. The market size is expected to grow gradually reaching 50% of the market in 2035. AUTOPILOT develops new services on top of IoT to involve autonomous driving vehicles, like autonomous car sharing, automated parking, or enhanced digital dynamic maps to allow fully autonomous driving. AUTOPILOT IoT enabled autonomous driving cars are tested, in real conditions, at four permanent large scale pilot sites in Finland, France, Netherlands and Italy, whose test results will allow multi-criteria evaluations (Technical, user, business, legal) of the IoT impact on pushing the level of autonomous driving.

[11] https://european-iot-pilots.eu/

IoF2020	IoF2020 (Internet of Food and Farm 2020) brings together 70 partners from 16 European countries with the objectives to accelerate adoption of IoT for securing sufficient, safe and healthy food and to strengthen competitiveness of farming and food chains in Europe. It will consolidate Europe's leading position in the global IoT industry by fostering a symbiotic ecosystem of farmers, food industry, technology providers and research institutes. The heart of the project is formed by 19 use cases grouped in 5 trials with end users from the Arable, Dairy, Fruits, Vegetables and Meat verticals and IoT integrators that demonstrate the business case of innovative IoT solutions for many application areas. A lean multi-actor approach focusing on user acceptability, stakeholder engagement and sustainable business models boost technology and market readiness levels and bring end user adoption to the next stage. This development is enhanced by an open IoT architecture and infrastructure of reusable components based on existing standards and a security and privacy framework.
MONICA	MONICA (Management Of Networked IoT Wearables – Very Large Scale Demonstration of Cultural Societal) brings together 28 partners from 9 European countries with the objectives to provide a very large-scale demonstration of multiple existing and new Internet of Things technologies for Smarter Living. The solution will be deployed in six major cities in Europe. MONICA demonstrates a large-scale IoT ecosystem that uses innovative wearable and portable IoT sensors and actuators with closed-loop back-end services integrated into an interoperable, cloud-based platform capable of offering a multitude of simultaneous, targeted applications. All ecosystems are demonstrated in the scope of large-scale city events but have general applicability for dynamically deploying Smart City applications in many fixed locations such as airports, main traffic arterials, and construction sites. Moreover, it is inherent in the MONICA approach to identify the official standardisation potential areas in all stages of the project.
SYNCHRONICITY	SYNCHRONICITY (Delivering an IoT enabled Digital Single Market for Europe and Beyond) brings together 33 partners from 9 European countries and 1 from South Korea with the objectives to deliver a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones – 8 European cities and 3 more worldwide cities. SYNCHRONICITY is working to establish a reference architecture for the envisioned IoT-enabled city marketplace with identified interoperability points and interfaces and data models for different verticals. This includes tools for co-creation & integration of legacy platforms & IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation on the market. SYNCHRONICITY pilots these foundations in the reference zones together with a set of citizen-centred services in three high-impact areas, showing the value to cities, businesses and citizens involved, linked directly to the global market.

3.2 Supporting the Large-Scale Pilots

With the support of two support actions (CREATE-IoT, U4IoT), a collaboration has taken place to foster the deployment of IoT solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions.

This includes:

- Mapping of pilot architecture approaches with validated IoT reference architectures,
- Contribution to strategic activity groups including security, privacy and trust, and
- Contribution to clustering results of horizontal nature such as interoperability, of standardisation.

Figure 2 shows the cooperation topics that have taken place. This deliverable focuses on results concerning security, privacy and trust.

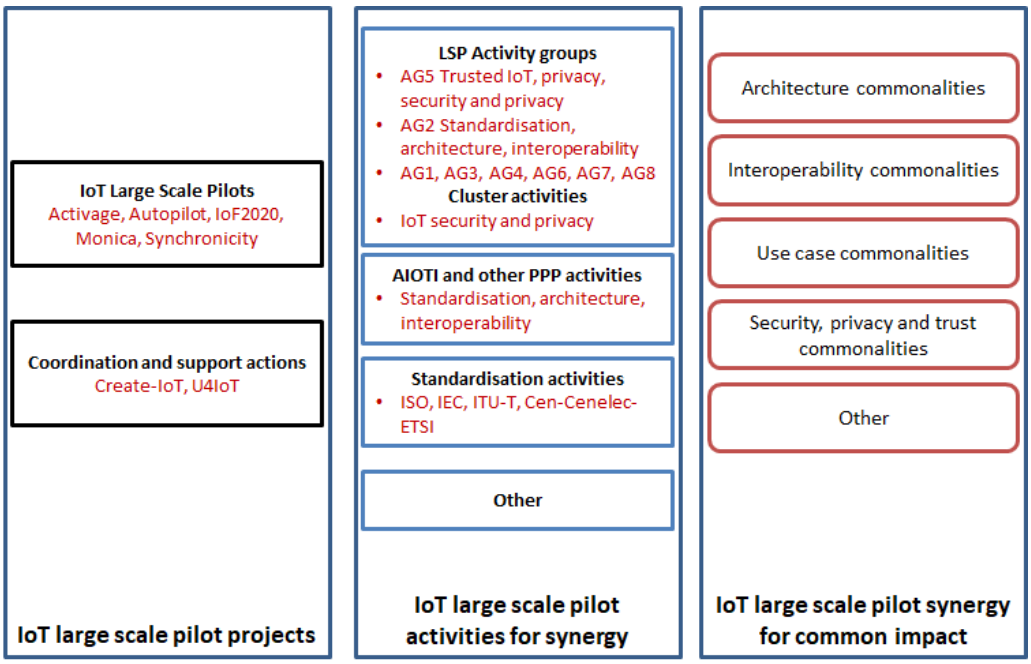


Figure 2: Cooperation within large-scale pilots and CSAs.

This deliverable will be useful to

- Further large-scale pilots. Figure 3 shows a list of further pilots that have started, and others are planned.
- The larger research community.
- A larger audience including industry, public administration and standardization bodies.

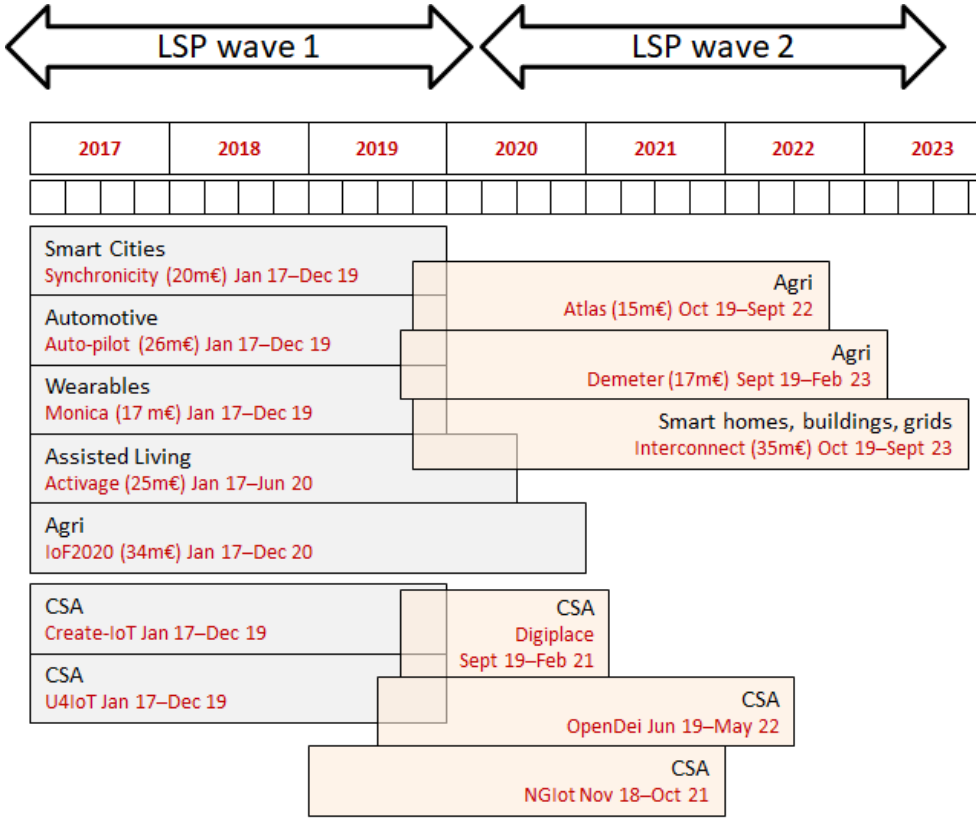


Figure 3: Waves of large-scale pilots.

Some of the results focusing on privacy has been integrated in a document under publication entitled "Good Practices for Personal Data Protection in Large-Scale Deployment of Internet of Things".

3.3 Standardisation Development

Since the start of the large-scale pilot program, the standardisation landscape has changed significantly. We list here the various related initiatives that have been carried out which may have an influence on an IoT policy framework.

ISO/IEC JTC1/SC38: SC38 is the committee focusing on cloud computing. This committee was established in 2009:

- ISO/IEC 23751 (Data sharing agreement (DSA) framework) was started in 2019. The standard is under development.

ISO/IEC JTC1/SC41: SC41 is the committee focusing on IoT. This committee was established in 2017. It is followed by AIOTI through a liaison category A[12]:

- ISO/IEC 30141 IoT reference architecture was published in 2018. It includes an entire section on IoT trustworthiness, covering safety, resilience, security and privacy. It makes the points that these concerns have an impact on the architecture of IoT systems.
- An ad-hoc group on trustworthiness was started in June 2017 which led to the development of ISO/IEC 30149 IoT Trustworthiness frameworks. This standard is under development.
- A definition of trustworthiness was proposed by the ad-hoc group: *deserving of trust or confidence*. A definition of IoT trustworthiness was provided: *Deserving trust within the entire lifecycle of an IoT implementation to ensure security, privacy, safety, reliability and resiliency.*
- In parallel, another standard development was started: ISO/IEC 30147 (Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes). ISO/IEC/IEEE 15288 is the standard on system lifecycle processes. This standard is under development.

ISO/IEC JTC1/SC42: SC42 is the committee focusing on AI. This committee was established in 2017. It is followed by BDVA through a liaison category A:

- A study group was created in May 2018 on trustworthiness, which led to the development of ISO/IEC 23894 (AI risk management), ISO/IEC 24027 (Bias in AI systems and AI aided decision making), ISO/IEC 24028 (Overview of trustworthiness in AI), ISO/IEC 24029-1 (Assessment of robustness of neural networks). These standards are under development.
- The study group was transformed into a working group (WG3) at the end of 2018.

ISO/IEC JTC1/SC27: SC27 is the committee focusing on information security, cybersecurity and privacy protection. This committee was established in 1989. It involves multiple H2020 liaisons category C[13]. The historical focus of the committee is on security and privacy, and one could consider that all these standards are part a trustworthiness framework. The IPEN wiki[14] provides a good overview of the current work. The following activities can be mentioned:

- A study was started in October 2018 on the impact of AI on privacy[15]. The study is still underway.
- The development of a standard on consent record information structure will start in 2020.
- The development of a standard on organisational privacy will start in 2020.
- ISO/IEC 20547-4 (Big data security and privacy) was started in 2015 and transferred in 2016 to SC27. The standard is under development.
- ISO/IEC 24391 (Security and privacy of IoT domotics) was started in 2019. The standard is under development.

[12] Liaison officer is Antonio Kung
[13] CREATE-IoT is part of the PRIPARE liaison with SC27/WG5
[14] Ipen.trialog.com
[15] Antonio Kung is the rapporteur of this study.

- ISO/IEC 24462 (Ontology for ICT trustworthiness assessment) will start in 2020. It is the result of a study that was started on July 2017. The development of this standard has been transferred to a new working group, ISO/IEC JTC1/WG13, created in November 2019.
- ISO/IEC 27030 (Security and privacy guidelines for IoT) was started in 2018[16]. The standard is under development.
- ISO/IEC 27550 (Privacy engineering for system life cycle processes)[17] was published in September 2019.
- ISO/IEC 27555 (Guidelines on Personally Identifiable Information Deletion) was started in 2019. The standard is under development.
- ISO/IEC 27556 (User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences)[18] was started in 2019. The standard is under development
- ISO/IEC 27570 (Privacy guidelines for smart cities) [19] was started in 2018. It includes a citizen engagement process. The standard will be published in 2020.
- ISO/IEC 27701 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines) was published in August 2019.

ISO/IEC JTC1/AG7 – WG13: further to a request from SC41 made in July 2017 to JTC1, a study of trustworthiness standardization across JTC1 entities was launched (ISO/IEC JTC1/AG8). It was decided to transform the activity group into a working group and to transfer to it the development of ISO/IEC 24462.

ISO/IEC JTC1/AG8: AG8 (Meta reference architecture and reference architecture for systems integration) was set up in November 2018. One objective of AG08 is to develop a document that contains a definition, concepts, processes, models, and templates on Meta Reference Architecture for Systems Integration entities. A workshop was organised in August 2019 on Montreal with the participation of several AIOTI/CREATE-IoT members[20], resulting in the creation of three reports (analysis of RA related standards, convergent RAs, and roadmap of common RA stack). One of the further goals of AG08 is to integrate the concept of trustworthiness into architecture concerns. This will be one of the topics for the AG8 second workshop that will take place in Brussels (1-4 September 2020).

ISO PC317: PC317 (privacy by design for consumer goods and services) was established at the end of 2018 in order to work in the ISO 31700 (privacy by design for consumer goods and services) standard. The H2020 PDP4E project has created a liaison with PC317. PC317 focuses on the consumer viewpoint.

ITU-T SG 20: The ITU-T Study Group 20 is in charge of standardisation related to the Internet of Things, as well as to smart cities and communities. In the context of the SG20, SYNCHRONICITY project has been actively engaged and has contributed to ITU standardization activities through several contributions. This work has led to the adoption of three new ongoing work items based on contributions submitted by MI:

- **Y.API4IOT**: a new Recommendation titled “Open data application programming interface (API) for IoT data in smart cities and communities” in charge of standardizing a set of open APIs for IoT data sharing in smart cities. The proposal is directly based on SynchroniCity data model and architecture.[21]

[16] Antonio Kung is a co-editor
[17] Antonio Kung is the Editor
[18] Antonio Kung is a co-editor
[19] Antonio Kung is the Editor
[20] Emmanuel Darmois, Antonio Kung, Arne Berre.
[21] Sébastien Ziegler is the lead Editor

- **Y.Sup.Pot_API4IOT**: is a supplement titled "Features of application programming interface (APIs) for IoT data in smart cities and communities". It complements the draft recommendation Y.API4IOT by providing an overview of the state of the art and more technical details on the SYNCHRONICITY architecture model implementation as well as complementary approaches such as FIWARE and SAREF.[22]
- **Y.Sup.AI4IoT**: is a supplement titled "Unlocking Internet of Things with Artificial Intelligence". It is a Supplement on Artificial Intelligence and the Sustainable Development Goals (SDGs). It is dedicated to the implementation of AI-based technologies across the IoT and smart city ecosystem. It also links various AI technologies to support the achievement of the Sustainable Development Goals (SDGs), especially SDG 11 (Sustainable Cities and Communities) and SDG 9 (Industry and Innovation). The main elements examined in this Supplement are:
  - The various technologies from which AI will facilitate smart city transformations;
  - The role played by AI in managing the data generated within the IoT realm and urban spaces;
  - The main benefits of adopting AI and delving into how this technology could be leveraged to attain the targets stipulated in the recently established Sustainable Development Goals (SDGs).[23]

ITU-T FG-DPM: The ITU-T focus group on data processing management[24] was established by ITU-T study group 20 in March 2017, and its work was completed in July 2017. Focus groups in ITU-T are open to non ITU-T members. The SYNCHRONICITY project was influential in the work carried out in the focus group. The focus group produced 15 deliverables all freely accessible. Concerning trustworthiness:

- A deliverable entitled "D4.1 Frameworks for security, privacy, risk and governance in data processing and management" was produced with major contributions from SYNCHRONICITY and CREATE-IoT.
- A deliverable entitled "D4.3 Overview of technical enablers for trusted data" was produced.
- A deliverable entitled "D2.1 Data Processing and Management Framework for IoT and Smart Cities and Communities" was developed with major contributions from SYNCHRONICITY and CREATE-IoT.
- A Deliverable "D0.1 Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary" was produced with major contributions from SYNCHRONICITY and CREATE-IoT.

ETSI TC Cyber and CEN-CENELEC JTC13: A joint document EN 303 645 (Cyber Security for Consumer Internet of Things) was published in January 2019, with a revision in November 2019[25]. This document follows the "code of practice for consumer IoT security" published by the department of digital, culture, media & sport[26] in the UK in October 2018.

ETSI has also published several technical reports related to IoT:

- In August 2019, SmartM2M; Teaching material; Part 1: Security[27],
- In October 2019, SmartM2M; Teaching material; Part 2: Privacy[28],

[22] Sébastien Ziegler is the lead Editor
[23] Sébastien Ziegler and Anna Brekine are the lead Editors
[24] https://www.itu.int/en/ITU-T/focusgroups/dpm/Pages/default.aspx
[25] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf
[26] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
[27] https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf

- In March 2019, User Group; User Centric Approach; Guidance for providers and standardization makers[29].

Many standardisation initiatives have taken place during the first wave of large-scale pilots, and it is likely that many other initiatives will take place in the next years. Since large-scale pilots' objective is to learn and prepare for fully fledge deployment, monitoring but also shaping standards is important. The whole large-scale pilots programme has benefited from the following support actions:

A. CREATE-IoT support action has an entire work package on standardisation (WP6)
B. The large-scale pilot program has a dedicated activity group on standardisation (AG02)
C. AIOTI has a specific working group on standardisation (WG3)
D. H2020 has specific a support action (StandICT) to support experts to standardisation. Further the annual multi-stakeholder platform (MSP) publishes a rolling plan that provides guidance on standardisation[30].

It is expected that beyond CREATE-IoT, A and B will be replaced by other support actions.

[28] https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf
[29] https://www.etsi.org/deliver/etsi_tr/103600_103699/103603/01.01.01_60/tr_103603v010101p.pdf
[30] https://ec.europa.eu/growth/industry/policy/ict-standardisation_en#rolling_plan_ict_standardisation

4. TRUST IN AN IOT POLICY FRAMEWORK

This chapter provides an overall analysis of trust in an IoT policy framework leveraging the work of the large-scale pilot program. It first summarises the main trusts concepts of the CREATE-IoT policy framework (D05.01). It then provides the viewpoint of standardisation on trust. It then provides the viewpoint of the large-scale pilots on trust. It finally provides an analysis integrating all viewpoints.

4.1 Input from D05.01

The below table summarizes the main trust concepts of the CREATE-IoT IoT policy framework as described in D05.01.

Table 5: Trust concepts

Concept	Description
Overall perspective	Complexity of interactions: • The concept of trust is highly complex with no definitive consensus. • Applied to IoT Systems one proposal is to decompose trust into device trust, entity trust and data trust. The complexity of interactions in an IoT systems calls for a focus on important interactions which can be identified as interfaces between relevant IoT architecture entities. Trust frameworks: • IoT bridges virtual, digital, physical worlds. • It must integrate security, safety, reliability, connectability, resilience, availability, dependability, privacy. • It includes a community vision (friendship, ownership, community).
Socio-economical perspective of trust	• Trust enhances economic efficiency under certain conditions. • An individual, societal or relationship viewpoint is needed, to ensure that economic transactions are mutually beneficial rather than exploitative.
Business perspective of trust	• IoT business subject to a series of adoption factors relevant for trust, such as reputation. • It is based on user's perception, and influenced by the social environment
Technical perspective of trust: components	• Includes society, technology, information, knowledge, users, humans. • Includes concerns (e.g. security, privacy, safety, …). • Enabled by processes.

4.2 Input from Standardisation

Table 6: Standardisation landscape on trust

Trust facet	
Socio-economical perspective	**Situation for IoT:** The integration of socio-economical perspective is not well developed at standardisation level, but they are tangible signs of interest: • ISO/IEC JT1/SC41 started an ad-hoc group on human factors, however the group was disbanded because of lack of participation. • AI is the domain where trustworthiness challenges have been recognized as important. ISO/IEC 24028 (Overview of trustworthiness in AI) lists new security and privacy threats as well as issues such as bias, unpredictability and opaqueness. ISO/IEC JTC1/SC27 is

	studying the impact of AI on privacy standards. • Privacy is a domain where user empowerment has been recognized as exemplified by ISO/IEC 27570 (privacy guidelines for smart cities)[31]. **Recommendations and opportunities for large scale projects:** Large scale pilots are invited to gain knowledge in the area of socio-economical perspective and contribute to standardization.
Business perspective	**Situation for IoT:** • Standardisation inherently contributes to trust since compliance to standards helps ensure more efficient business. • Standards focusing on trustworthiness properties (safety, security, privacy, resilience, etc.) are often built upon three pillars: impact or risk assessment, measures and assurance. Such standards are effective when they are adopted and practiced. This has been very effective in the security of information systems (ISO/IEC 27X series), and in security products (ISO/IEC 15408 common criteria). The recently published 27701 standard on privacy is likely to be also very effective. • There is no such standard on trustworthiness yet. This is because having a consensus on the concept of trust is complex and having an agreement on an effective assurance approach is also challenging. • IoT systems can involve complex ecosystems of stakeholders. Standards for helping them to collaborate towards common goals are lacking. Privacy, security, safety, resilience is not just a problem of one organisation. It is a collaborative undertaking that might require some governance. Standardisation includes attempts to address this point. AIOTI contributed a report on standard for ecosystems to ISO/IEC SC41 in 2018. ISO/IEC 27570 (privacy guidelines for smart cities) or ISO/IEC 23751 (Data sharing agreement (DSA) frameworks) do address ecosystems. **Recommendations and opportunities for large scale projects:** Research and innovation projects and large-scale pilots will gain further knowledge on trustworthiness. They are invited to continue contributions in this area.
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	**Situation for IoT:** • ISO/IEC 30141 (IoT reference architecture) covers safety, security, privacy, reliability and resilience but it stays at the principle level and does not provide guidelines on how trustworthiness can be integrated • Attempts for integration do happen on a "bilateral basis". For instance, privacy is rather well integrated with security (as both concerns are dealt by the same SC27 committee). On the other hand, safety is not well integrated with security (as safety is dealt within domain specific standards). • The integration of trustworthiness properties is an architecture issue. AIOTI and CREATE-IoT have been instrumental[32] to shape an approach to integrate trustworthiness in architecture considerations (within ISO/IEC JTC1/AG9) **Recommendations and opportunities for large scale projects:** Architects in research and innovation projects and large-scale pilot should gain knowledge on the properties of trustworthiness. They are invited to provide feedback on this topic, in particular on the integration of trustworthiness into architecture work (a workshop will be organised in Brussels on September 1-4th, 2020)

4.3 Input from Large-Scale Pilots

4.3.1 ACTIVAGE

The input in this section is taken from specific contributions, deliverables from the ACTIVAGE project, as well as from the 2018 publication entitled "Next Generation Internet of Things. Distributed Intelligence and the Edge and Human Machine-to-Machine Cooperation" [33]

[31] Editors are Antonio Kung (Create-IoT) and Heung Youl Youm (Korea, Chair of ITU-T SG17)

[32] See https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf. This deliverable has been presented to ISO/IEC JTC1/AG8.

Table 7: ACTIVAGE feedback on trust

Trust facet	
Socio-economical perspective	A parameter that could raise moral issues is the equal access in IoT environments and its benefits. According to diverse users' capabilities access is not always a democratic and equal process. On the contrary it poses limits to a part of community not being familiarized with emerging technologies[34].
Business perspective	ACTIVAGE is an LSP that brings together the IoT and AHA communities to demonstrate the value of the first with respect to successful implementations of AHA solutions in terms of quality of life (QoL) for Citizens, sustainability of Health and Social Care systems and Economical and industrial growth in Europe.
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	Security issues emerge according to IoT architecture, protocols used for networking, communication, and the overall management. In particular regarding trust evaluation, data integrity and traceability concerns have to be taken into account along with potential threats and attacks. Referring more specifically at many IoT devices, fall back plans and mechanisms to introduce a tamper-proof environment are needed. Finally, the decentralised technology of Blockchain has been so far indicated by the relevant research community as a key enabler for network security and trust[35]. As stated in the 2018 publication cited above, secure IoT systems with high-level of personal data protection are mandatory to keep the users' trust. These aspects are essential to deploy massively the IoT technology in the coming years

4.3.2 AUTOPILOT

Table 8: AUTOPILOT feedback on trust

Trust facet	
Socio-economical perspective	The social and economic implications of autonomous vehicle technologies affect all the stakeholders in the new created autonomous vehicles and IoT ecosystem. The significance of these implications will play an important role in the future of autonomous vehicles among consumers. As autonomous vehicles, IoT, and AI connected systems are deployed, they increasingly rely on information that is exchanged in order to perform and conduct their safety-critical operations. Keeping such systems (and the information within) trustworthy, secure, safe, private for the required cases is a critical element for the public acceptance and adoption of such autonomous systems. Challenges include legislative issues in order to identify the accountability in case of incidents and malfunction, provide technologies like software, hardware, communication, security to assure 100% reliable systems to avoid technical mistakes, provide solutions to protect the vehicles from cyber-attacks and external interference, implement mechanisms to protect the privacy of the owners/users/pedestrians and address ethical issue such as the vehicle behaviour model in an inevitable collision (e.g., to hit a pedestrian or to drive a vehicle off the road where passengers may be in danger).
Business perspective	The autonomous vehicles are expected to bring significant benefits in terms of fuel efficiency, reduced emissions, saving time and safer mobility. However, consumers' trust in the autonomous vehicle technologies, services and applications need to be significantly increased before they are ready for a fully autonomous future. Trust in autonomous technology is the key to a driverless future and for any business models that implements the technology. The decline in the frequency of accidents will affect the mix of insurance as commercial and products liability lines expand. The introduction of sharing mobility based on autonomous vehicles and the elimination of excess capacity could bring severe market issues, with changing business models and new competitors entering the market. As trust becomes a key issue from the business perspective, the automotive functional safety is evolving from fail-safe to fail-operational architectures.

[33] Chapter 4 of https://european-iot-pilots.eu/next-generation-internet-of-things-distributed-intelligence-at-the-edge-and-human-machine-to-machine-cooperation/

[34] ACTIVAGE D1.5 Ethics and Privacy Protection Manual

[35] Khan, M. A., & Salah, K. (2018). IoT security: Review, Blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	The autonomous vehicles and IoT Trust Framework adopted by AUTOPILOT provides a set of principles and the underlying structure that exhibit the trustworthiness, dependability and privacy for autonomous vehicles and IoT solutions into a holistic manner. The framework integrates the concepts of availability, reliability, safety, security, resilience, privacy and sustainability best practices, embracing "privacy and security by design" as a model for an implementable autonomous vehicle and IoT code of conduct and engagement. Trustworthiness is a property of people that engenders trust in the autonomous vehicles system, including IoT technologies. If the user has a choice to use one service or another, decision will depend of the degree of trustworthiness that the user has on the service. Dependability in complex autonomous vehicles, IoT and AI system represents the degree to which the system can perform its required function at any randomly chosen time during its specified operating period, disregarding non-operation related influences. In this context security, safety, reliability, connectability, resilience, availability properties are presented as integrated part of the dependability and trustworthiness concepts.

4.3.3 MONICA

Table 9: MONICA feedback on trust

Trust facet	
Socio-economical perspective	MONICA leverages • An initiative launched by the European Commission called CAPS, which stands for Collective Awareness Platform for Sustainability and Social Innovation[36]. The objective is to try out new engagement models that can help solve emerging sustainability problems. The models are based on creating awareness of environmental or societal challenges through an online platform by displaying facts and information. Based on this, the aim is to foster solutions through collective action and social innovation, i.e., creating new ideas together to improve a situation[37]. There is one such CAP per city. • Citizen engagement through different schemes such as involving citizens in the value creation by being active collectors of the data (in Copenhagen), or through user engagement strategies with hackathon (in Torino) The collective awareness platform for citizen engagement and co-creativity is the crux for trust in a smart city.
Business perspective	The CAPs thereby complement existing initiatives that support citizen involvement in the utilisation of open data. Both Copenhagen and Torino have planned to integrate data from various open data platforms into the CAP and also enable access to new open data coming from the MONICA project. This will allow for improved efficiency of public services, and economic growth to social welfare. As stated in the case of Copenhagen, "the city expects to make the citizens aware of problems, and thereby also interested in potential solutions. The City hopes to inspire citizens to act". The purpose of the CAP is to present knowledge in a new way, and thereby gain insight which might be used to identify potential solutions. Thus, it might inspire entrepreneurs to develop new solutions based on the data, it might point to new knowledge benefitting city planning, and it might facilitate new citizen initiatives on improvement.
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	The main concerns for trustworthiness properties are as follows in MONICA: • The supporting applications for city events focus on the security and safety of citizens participating to these events. • Collection and use data must meet security and privacy requirements. One objective of the demonstration of IoT technologies is to develop and deploy a generic data security, privacy and trust Framework that ensures full data protection and privacy and allows role-based control measures to enforce information exchange only among authenticated and authorised entities[38].

[36] https://ec.europa.eu/digital-single-market/collective-awareness
[37] MONICA deliverable. D11.1 Collective Awareness Platform for Citizen Engagement and Co-creativity
[38] MONICA deliverable D9.1_Impact_Assessment_and_Validation_Framework_v1.0

4.3.4 IoF2020

The analysis of IoF2020 to provide feedback on IoF2020 comes from the deliverables published on their LSP web site[39] with specific attention to D7.1 Literature review.

Table 10: IoF2020 feedback on trust

Trust facet	
Socio-economical perspective	There are great opportunities in smart farming to benefit from IoT control, monitoring and big data to be more productive, deliver higher yields, reduce waste, be more transparent to the public and improve food security. There are many factors that arise that have to be considered when stakeholders may prioritise productivity to increase yields and profits and to the detriment of ecological footprint and animal welfare. Making use of the data that smart farming generates will likely favour the larger farm businesses and new entrants that understand digital technologies that are able to invest in IoT to monitor and control farming processes and thus has high risk of creating a digital divide impacting negatively on smaller sole trader farmers.
Business perspective	Sharing of farm data for analysis with agricultural technology providers (ATPs) offering consultancy services can provide beneficial feedback and insightful recommendations to farmers. However, there is risk that same ATP or ATP partner entities of other farm services, such as seed suppliers, could benefit from this inside information to potentially discriminate against the farmer.
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	It is expected that there will be increased public transparency in farms, traceability and increased food security. Farm data is seen as commercially sensitive in many cases such as crop yield, soil fertility etc. and it is needed to have contractual clarity on how the farm data is processed by third parties and if it is shared for other uses. There is also a risk of the monitoring technologies being used by larger corporates to control the farmers employed and create profiles that can be used to discriminate the farmers.

4.3.5 SYNCHRONICITY

Table 11: SYNCHRONICITY feedback on trust

Trust facet	
Socio-economical perspective	SYNCHRONICITY is a project on smart-cities and therefore this context needs to be considered. It is based on the belief that creating a simplified, open and agile digital market across borders will help cities and its citizens to get better services. It will also help businesses of all sizes transparently compete and easily scale their products and solutions. All this together will enable the identification and development of agile city standards that will allow establishing an effective marketplace for all. The project represents the first attempt to deliver a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones, 8 European cities and 3 more worldwide cities, connecting 34 partners from 11 countries and 4 continents.
Business perspective	The deliverable 1.3 identifies relevant market barriers for the smart city market. The listed barriers are: • Lack of standardized multi-vendor ecosystem; • Lack of common service provisioning environments across cities; • Close coupling of IoT infrastructure and applications (IoT silos); • Lack of tools, license models, and platforms to facilitate the incentivized sharing of urban IoT data and other relevant data sets; • Lack of harmonized business practice and legal frameworks across cities; • Lack of understanding of privacy and personal data protection implications; • Lack of confidence in adopting emerging technologies due to increasing technology

[39] https://www.iof2020.eu/about/deliverables

	fluidity. The key identified non-technical barriers included: • Economical costs and budget constraints; • Frequent political changes and lack of continuity; • Lack of involvement of citizens; • Lack of a holistic smart city strategy. The identified barriers revealed a large fragmentation across different cities and a lack of coherent support mechanisms that make a common addressable market to emerge. In order to overcome these barriers, a digital single market should exhibit the following properties: • Interoperability; • Free competition of vendors and solution providers; • Common service environments; • IoT infrastructure re-use; • Trusted participation of the IoT data providers and consumers; Incentivized data sharing; • Common legal foundation.
Properties (e.g. Security, Safety, Reliability, Connectability, Resilience, Availability)	Overcoming the barriers identified requires a common approach across the different cities. This approach needs to consider of the following elements: 1. A common reference architecture for smart city platforms. A standardized reference architecture, which is widely adopted among cities with clearly defined components and interfaces, is fundamental to overcome vendor lock-in. It will boost market confidence and lay down the foundations for the required economies of scale. 2. Common northbound interface. Developers require a common, homogeneous and IoT independent way to access data from devices infrastructure, but also from any other subsystem in the city that can provide valuable information to develop smart services and applications. More specifically, this includes a) a common standard API for context information management; b) a common set of information models enabling actual interoperability applications; c) a set of common standards data publication platforms have to comply with, enabling the harvesting of data coming from multiple federated platforms as well as the publication of real-time open data. 3. Common southbound interface. For IoT device vendors and manufacturers it should become easier to offer suitable device stacks for integrating heterogeneous IoT components into a common environment, together with a marketplace for compliant IoT products and solutions. 4. Market place enablers that encourage sharing of urban IoT data and other relevant data sets among different stakeholders. By providing a marketplace as a one-stop-shop, it will become much easier for data consumers to discover and access urban data sources. The availability of a trusted marketplace with monetization mechanisms will allow third parties to generate easier revenue streams from their urban data sources. This will encourage more businesses to share currently closed data sources or incentivize deployments of new IoT infrastructure as secondary revenue streams can be generated, making more business cases viable. Data consumers may not require lengthy negotiations of license terms as data license terms can be negotiated from pre-configured options of the provided on the fly.

4.4 Resulting Analysis

The table below shows the resulting recommendations for trust in an IoT policy framework.

Table 12: Recommendations for Trust in an IoT policy framework

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: ○ IoT bridges the virtual/digital world with the physical world, ○ IoT covers complex interactions in an ecosystem, and ○ IoT is based on complex architecture considerations that have to integrate technical properties such as security, safety, reliability, connectability, resilience, availability, dependability, privacy.		
Socio-economic	Overall position	Socio-economic policies should include measures to enable economic progress associated with social progress.

perspective		A trustworthy IoT environment must therefore cover business operations associated with social processes.
	Standardisation viewpoint	The integration of socio-economic viewpoint is not well developed at standardisation level. Large scale pilots are invited to contribute to this integration in standards.
	Assisted living viewpoint	Socio-economic policies should include measures for equal access to IoT environments and its benefits.
	Autonomous vehicle viewpoint	Autonomous vehicle technologies involve complex capabilities (IoT, AI) used in safety-critical operations. Keeping such systems trustworthy is critical for public acceptance in a domain. Furthermore, many legal issues are still to be addressed. Socio-economic policies should include measures for trustworthiness of complex systems and agile update of new legal issues.
	Wearable viewpoint	Socio-economic policies should include measures for citizen engagement and co-creation.
	Agrifood viewpoint	To make sure that smart farming does not just concentrate on increased productivity there can be policies in place that also set ecological goals and identify how to encourage/incentivise farmers to make additional use of IoT to work towards these goals. Additionally, care must be taken not to create a digital divide in the farming community, and this is another area where policy measures can be considered to address this.
	Smart city viewpoint	Socio-economic policies should include measures for easy access to smart cities IoT market by local and/or small business stakeholders.
Business perspective	Overall position	Business policies should include measure integrating factors relevant for trust, such as reputation, taking into account user's perception and the social environment.
	Standardisation viewpoint	Business policies should include measures to create and adopt standards in the area of trust. They will be key enablers for the advent of IoT. Large scale pilots are invited to gain knowledge in the area of trustworthiness and contribute to standardization.
	Assisted living viewpoint	Business policies should include measures to foster quality of life (QoL) for citizens while ensuring the sustainability of health and social care systems and economical and industrial growth in Europe.
	Autonomous vehicle viewpoint	The business perspective for autonomous vehicles is related to benefits in terms of fuel efficiency, reduced emissions, saving time and safer mobility. The introduction of sharing mobility based on autonomous vehicles and the elimination of excess capacity will also change the market. To enable this, business policies should include measure to ensure consumers' trust in the autonomous vehicle technologies.
	Wearable viewpoint	Business policies should include measures for open data as an instrument to facilitate citizen led entrepreneurship as well as city planning.
	Agrifood viewpoint	Open market policies should be addressed so that Agricultural Technology Providers (ATPs) that provide analysis of farm data are not unfairly using the data to give other related business areas unfair advantages in targeting farmers or to discriminate against them. "*In IoT, data is very important; data is created, shared and needs to be protected. The right framework must be provided, and full control of the data owner ensured." Ref D3.4 Policy Recommendations.*
	Smart city viewpoint	Business policies should include measures to remove barriers for the smart city markets, focusing on interoperability, free competition, common service environments, IoT infrastructure re-use, trusted participation of IoT data providers and consumers, incentivized data sharing and common legal foundation.
Technical perspective	Overall position	Technical policies should leverage an agreed architecture description and terminology that can be based on current work in the IoT community. Deliverable D06.02

		(Recommendations for commonalities and interoperability profiles of IoT platforms)[40] suggests a 3D model based on layers, cross-cutting functions, and properties. They will have to identify the elements to which trust should be achieved (e.g. device trust, system trust, data trust).
	Standardisation viewpoint	Technical policies should include measures to define standards providing guidance on the engineering of trust. Architects in research and innovation projects and large-scale pilot should gain knowledge on the properties of trustworthiness. They are invited to provide feedback on this topic, in particular on the integration of trustworthiness into architecture work (a workshop will be organised in Brussels on September 1-4th, 2020).
	Assisted living viewpoint	Technical policies should include measures for cross-cutting capabilities on data integrity, traceability, tamper proof environment and high level of personal data protection.
	Autonomous vehicle viewpoint	Technical policies should include measures for trust assurance, based on the concept of degree of trustworthiness that the user has on a service. This will allow for the evaluation of the dependability to a complex autonomous vehicle, or the degree to which the system can perform its required function.
	Wearable viewpoint	Technical policies should include measures to for generic implementation of cross-cutting capabilities such as role-based control measures for data security, privacy and trust.
	Agrifood viewpoint	Technical policies should be in place to make sure that specific commercially sensitive farm data is stored and processed securely and is not shared with others without consent and if anonymised for big data purposes that there is no risk of re-identifying the specific farm.
	Smart city viewpoint	Technical policies should include measures for system interoperability: common reference architecture, common northbound and southbound interface, as well as measures for reuse (marketplace enablers).

[40] https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf

5. ENGAGEMENT IN AN IOT POLICY FRAMEWORK

This chapter provides an overall analysis of organisation engagement in an IoT policy framework leveraging the work of the large-scale pilot program. It first summarises the main engagements concepts of the CREATE-IoT policy framework. It then provides the viewpoint of standardisation on engagement. It then provides the viewpoint of the large-scale pilots. It finally provides an analysis integrating all viewpoints.

5.1 Input from D05.01

The below table summarizes the main engagement concepts of the CREATE-IoT IoT policy framework as described in D05.01. Note that this covers the engagement of organisations involved in an IoT initiative. It does not cover the issue of citizen engagement which is included in the security and privacy framework in the next section.

Table 13: Engagement concepts

Concept	Description
Engagement on ethics	• Business Ethics and, more specifically, Corporate Social Responsibility are highly relevant for the IoT environment. • IoT is considered to be one of the main technological trends, triggering concerns of ethical nature.
Engagement on standards	• Standardization constitute a form of soft regulation that can influence the behaviour for organizations active in the domain of technologies.
Engagement on legislation	• Regulation imposes stakeholders' engagement due to their mandatory nature. Influential regulations to be considered by IoT systems operators are GDPR, the NIS directive, the ePrivacy directive, and the cybersecurity act.
Engagement on contracts	• An IoT ecosystem includes many stakeholders. A contractual relationship must be settled between them.

5.2 Input from Standardisation

Table 14: Standardisation landscape on engagement

Engagement facet	
Engagement on ethics	**Situation for IoT:** • ISO 26000 guidance on social responsibility provides good overall corporate guidance. ISO 17033 provides guidance on ethical claims. • To our knowledge there is no specific standard on ethics for ICT. Note that the H2020 Sherpa project[41] has prepared a contribution on ethics that will be submitted to the SC27 study on the impact of AI to privacy. **Recommendations and opportunities for large scale projects:** Research and innovation projects and large-scale pilots have an opportunity to contribute in this area with the support of other H2020 projects such as Sherpa.
Engagement on standards	**Situation for IoT:** • The use of standards is on voluntary basis. • Standards associated with assurance or certification schemes are needed for interoperability. • Standards associated with assurance or certification schemes will be needed for trustworthiness. There are certification schemes for security (e.g. 27x, 15408), and it is

[41] Shaping the Ethical Dimensions of Smart Information Systems: a European Perspective https://www.project-sherpa.eu/

	likely that there will be a certification scheme for privacy information management systems, but there is need for consensus on trustworthiness assurance. **Recommendations and opportunities for large scale projects:** Research and innovation projects and large-scale pilots have an opportunity to contribute in the area of trustworthiness assurance.
Engagement on legislation	**Situation for IoT:** Standards do not cover legislation. However, the advent of GDPR has profoundly influenced the list of privacy standards[42]. Some standards for instance ISO/IEC 27701 do contain an annex on GDPR. **Recommendations and opportunities for large scale projects:** Research and innovation projects and large-scale pilots should monitor and possibly contribute to such documents.
Engagement on contracts	**Situation for IoT:** The advent of IoT ecosystem will require agreement frameworks. ISO/IEC 23751 (data sharing agreement (DSA) frameworks) is an example of such undertaking. Smart contracts based on Blockchain are also likely to lead to standards. **Recommendations and opportunities for large scale projects:** Research and innovation projects and large-scale pilots should monitor and possibly contribute to such types of standards.

5.3 Input from Large Scale Pilots

5.3.1 ACTIVAGE

The input in this section is taken from specific contributions, deliverables from the ACTIVAGE project, as well as from the publication entitled "Next Generation Internet of Things. Distributed Intelligence and the Edge and Human Machine-to-Machine Cooperation" [43]

Table 15: ACTIVAGE feedback on engagement

Engagement facet	
Engagement on ethics	The obtrusiveness and visibility of health-related devices could affect user acceptance and future use[44]. Moreover, ethics can be considered from the perspective of data and also practice level. General principles as laws and regulations awareness, data proportionality and individual empowerment on data control (data proportionality) could define a framework for individuals' rights' maintenance. However, the key component to health-related technologies is ethical assessment[45]. Users' data ethics and relevant policies seem to be clearly defined but in the landscape of IoT ecosystems, data ownership requires sufficient practices specifically in cases of cross-border data centres[46].
Engagement on standards	Here is ACTIVAGE analysis (done in 2018): • There are not official guidelines available for trust of IoT devices, in addition, there is no regulatory compliance defined for minimum security requirements. Despite the existence of many security guidelines in general, the literature lacks primary guidelines to help adopt security measures and standards for the IoT systems. • IoT systems use generally different wireless connectivity solutions not compliant with existing security standards.

[42] See ipen.trialog.com for an updated list of privacy standards

[43] Chapter 4 of https://european-iot-pilots.eu/next-generation-internet-of-things-distributed-intelligence-at-the-edge-and-human-machine-to-machine-cooperation/

[44] De Bleser, L., De Geest, S., Vincke, B., Ruppar, T., Vanhaecke, J., & Dobbels, F. (2011). How to test electronic adherence monitoring devices for use in daily life: a conceptual framework. *CIN: Computers, informatics, nursing*, *29*(9), 489-495.

[45] Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*, *19*(3), 157-175.

[46] ACTIVAGE D1.4 Data Management Plan

Engagement on legislation	N/A.
Engagement on contracts	Engagement on contracts has not been relevant since it has been superseded by the H2020 contract with the EC, or open call contracts.

5.3.2 AUTOPILOT

Table 16: AUTOPILOT feedback on engagement

Engagement facet	
Engagement on ethics	There are several facets of the ethical issues related to autonomous vehicles and IoT as the new technologies can fall under different classes of laws, and different ethical questions have to be raised. The AUTOPILOT focus was to use IoT technologies to support automated driving functions and increase safety in order that automated vehicles minimize casualties in all situations.
Engagement on standards	AUTOPILOT deliverable D5.8 (Standards and conformance of AD) provides an overview of the activities and results achieved by the AUTOPILOT Task 5.5 (Standardisation). During the lifetime of the project more than 25 contributions based on the activities carried out in AUTOPILOT have been submitted to SDOs. A comprehensive list of the activities is provided in AUTOPILOT delivery D5.7 (Standardisation Plan). AUTOPILOT has followed the overall autonomous vehicles readiness index results and the ranking of different countries around the world, based on four different criteria: policy and legislation, technology and innovation, infrastructure and consumer acceptance, prepared by KPMG and checked the different findings on the countries where the test sites and pilots were implemented.
Engagement on legislation	Autonomous vehicle legislation is essential for the development of the autonomous vehicle and IoT technologies. AUTOPILOT consortium has followed closely the legislative landscape at the European and MSs level and kept an open dialog with PAs on the legislation and the needs for experimentation, testing and deployment. As result AUTOPILOT delivery D5.4 has dedicated a chapter for an overview on the autonomous vehicles legislation.
Engagement on contracts	Engagement on contracts has not been relevant since it has been superseded by the H2020 contract with the EC.

5.3.3 MONICA

Table 17: MONICA feedback on engagement

Engagement facet	
Engagement on ethics	MONICA has produced two deliverables • MONICA ethical guidelines[47]. An important point is whether the informed consent, if any, covers the intended use of the data including long term preservation. • MONICA data management plan[48]. This plan includes a template that must be filled out by stakeholders. It includes a section on ethical aspects for each application. Examples of applications where ethical issues where identified are the following: • The surveillance video application. Local storage of video has to follow the ethical guidelines and the local regulations and laws for the site. • The wearable positioning streams application (UWB wristbands provide a stream of position information that is used for locating people for different purposes). Collected data may contain possible sensitive information about individual people movement. • The common operational picture application (The Common Operational Picture is the most central data element in MONICA. It represents the current status of all relevant operations and process parameters at the event site such as number of visitors, current reported incidents, threat levels, sound levels, etc. Data is accessed and used by event operators and security personnel). Data collected can contain sensitive data linking individuals to location

[47] In MONICA deliverable D10.5 MONICA Ethical Guidelines. This deliverable is not public
[48] See MONICA deliverable D11.2-Open-Data-Management-Plan-1.0

	and actions.
Engagement on standards	MONICA has actively monitored standards related to the IoT demonstrators[49], in particular on harmonized radio communication standards.
Engagement on legislation	As stated in MONICA deliverable D12.5, it was initially "decided to deploy a drone overhead of the pilot event area, in order to carry radio connected sensors picking up meteorological data for the ASFC real time sound field calculations, video signal for the crowd monitoring and a microphone, streaming the audio above the event for the acoustic loop. Having studied the current non-harmonized (national only) drone regulation across Europe, technical as well as safety related, it was decided to select a much more safe and in some technical aspects more elegant solution, in the form of a tethered (line connected to the ground) soft air balloon (a so-called "blimp") to carry the small pieces of sensor equipment. Such small airship is not running out of power, and does not create propeller noise, which would have to be filtered out of the digital audio stream from the on-board microphone."
Engagement on contracts	Engagement on contracts has not been relevant since it has been superseded by the H2020 contract with the EC.

5.3.4 IoF2020

Table 18: IoF2020 feedback on engagement

Engagement facet	
Engagement on ethics	IOF2020 has a work package dedicated to Ethics and Responsible Design Innovation. However, the deliverables are not yet published, apart from one D7.1 deliverable "*Ethics of smart farming: Current questions and directions for responsible innovation towards the future*". The other deliverables will be finalized during 2020 and will be publically available. As can be seen by the D7.1, current ethical discussion about smart farming circles around three themes: (1) data ownership and data access, (2) distribution of power and (3) impacts on human life and society.
Engagement on standards	Task 3.2 of WP 3 addresses the IoT Standardisation objectives of IoF2020. The deliverable D3.5: Guidelines for the use of IoT related Standards in Smart Farming and Food Security provides recommendations that derive from a heterogeneous field of technological interactions. *"IoF2020 suggests that policy makers encourage voluntary standardisation, making it a crucial element within activities and ensure that they are freely available and can be used without additional cost".*
Engagement on legislation	Trust in data sharing, data access, data ownership and data protection are key issues identified by the use cases of IoF2020. Clear rules and understandable guidance must be given to famers and other stakeholders in the agricultural chain.
Engagement on contracts	Engagement on contracts has not been relevant since it has been superseded by the H2020 contract with the EC.

5.3.5 SYNCHRONICITY

Table 19: SYNCHRONICITY feedback on engagement

Engagement facet	
Engagement on ethics	This has been considered in the context of open data access and data protection. One important aspect not well considered in the engagement facet is the involvement of the citizen. The project has applied the following process: • collecting the needs of the different reference zones in terms of co-creation and guidance methodologies and tools to apply in order to successfully perform pilots with citizens and stakeholders, • building on existing citizen-centred models and tools, successfully applied in different contexts, in order to establish a solid framework on co-creation approaches within smart-

[49] See MONICA deliverable D12.5 Report on Standards Regulations and Policies for IoT Platforms_V1.0

	cities environments; and • providing guidance to reference zones so as to concretely and easily identify which co-creation methodologies should be implemented within the use cases exploited by the cities. This process is strictly connected both to engagement of citizens and stakeholders in defining the services that have developed within SYNCHRONICITY for the data marketplace and consequent platforms' deployment and operations. Co-creation methodologies have been also put in place for validating the services piloted in the reference zones, both at users, stakeholders, SMEs and citizens' level.
Engagement on standards	SYNCHRONICITY has been one of the most active projects on standardisation, focusing on smart cities related standards. Activities of the project have been reported in a project deliverable (D6.2 Internet of Things Standardization report), specifically to ITU-T in the Study Group 20, ETSI, OASC, IEEE, ESPRESSO and EIP-SCC in the framework of the SYNCHRONICITY project: • In September 2017, the ITU Study Group 20 approved the creation of a new work item titled "Open data application programming interface (API) for IoT data in smart cities and communities" with the reference Y.API4IOT. Mandat International was designated as Editor of the draft Recommendation with the support of several international delegations. The work includes a draft supplement on Artificial intelligence and sustainable development goals (SDGs) • ITU established a dedicated Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM in March 2017. • OASC has started a program on the concept of MIMS (Minimum interoperable mechanisms), including certification mechanisms. • Participation to various undertakings at ETSI level, including contribution to the ISG for cross-cutting context information management (and work related to NGSI-LD API), and contribution to the ETSI STF 566 (SAREF extensions for smart cities)
Engagement on legislation	Work has been done on licenses. This category is about the licenses and policies related to the use and access of data, services or applications within the marketplace. SYNCHRONICITY strives to create an ecosystem where all possible business models are enabled. So, there is a need for maximum flexibility regarding the licensing and policy models that can associated with the assets.
Engagement on contracts	Engagement on contracts has not been relevant since it has been superseded by the H2020 contract with the EC, or open call contracts.

5.4 Resulting Analysis

The table below shows the resulting recommendations for organisation engagement in an IoT policy framework.

Table 20: Recommendations for organisation engagement in an IoT policy framework

Organisation engagement is a key prerequisite for successful IoT. A IoT policy framework should include: • Measures for ethics engagement. • Measures for standardisation engagement. • Measures for legislation engagement. • Measures for contracts engagement.		
Engagement on ethics	Overall position	Practice for business ethics and corporate social responsibility should be carried out as they are highly relevant for the IoT environment.
	Standardisation viewpoint	Policies should include contribution and adoption of standards on ethics.
	Assisted living viewpoint	Policies should include measures for systematic ethical impact assessment of applications, user empowerment for health personal data, and protection in case of cross-border exchange.
	Autonomous vehicle viewpoint	Policies should include measures to update autonomous vehicles decision algorithms when use cases raising ethical issues lead to modification requirements.
	Wearable	Policies should include measures for systematic ethical impact assessment of

	viewpoint	applications.
	Agrifood viewpoint	Policies should include measures for the involvement of farmers using Responsible Research and Innovation methods to enhance their reflection about the future and gather their input on how to shape the technology (to fit farming practices and foster trust in them).
	Smart city viewpoint	Policies should include measures for the involvement of citizens using user-centred methods and co-creation.
Engagement on standards	Overall position	Standardization is a form of soft regulation that can influence the behaviour for organizations active in the domain of technologies.
	Standardisation viewpoint	Policies should include measures to foster the contribution and adoption of standards related to trust: assessment, measures, assurance.
	Assisted living viewpoint	Policies should include measures for the production of guidelines on trust.
	Autonomous vehicle viewpoint	Policies should include measures to monitor the evolution of standards and contribute to them in the domain.
	Wearable viewpoint	Policies should include measures to monitor and contribute to wireless communication standards.
	Agrifood viewpoint	Policies should include measures to keep data available in data platforms for (re-) use by different stakeholders such as researchers, policymakers, ICT companies, farmers etc. Careful reflection should go into the governance of these platforms and stakeholders should have a role in that.
	Smart city viewpoint	Policies should include measures to create the wealth of standards needed to create an open market for smart cities.
Engagement on legislation	Overall position	Policies should include measures to monitor the evolution of legislation related to IoT on security and privacy.
	Standardisation viewpoint	Policies should include measures to study and clarify the relationship between standards and law.
	Assisted living viewpoint	Policies should consider ways to mitigate the power differences that are coming about as an effect of digitalisation of agriculture, as some have access to digital technologies and others don't, and some have digital knowledge and expertise to do something with data and others don't.
	Autonomous vehicle viewpoint	Policies should include measures to monitor legislation in the making for autonomous vehicles.
	Wearable viewpoint	Policies should include measure for legal impact assessment, possibly leading to alternate solutions.
	Agrifood viewpoint	Policies should consider ways to mitigate the power differences that are coming about as an effect of digitalisation of agriculture, as some have access to digital technologies and others don't, and some have digital knowledge and expertise to do something with data and others don't
	Smart city viewpoint	Policies should include measures on licenses for using and accessing data.
Engagement on contracts	Overall position	The advent of IoT ecosystems will require agreement frameworks. Research and innovation projects and large-scale pilots should monitor and possibly contribute to contractual practice.
	Standardisation viewpoint	Research and innovation projects and large-scale pilots should monitor and possibly contribute to agreement standards.

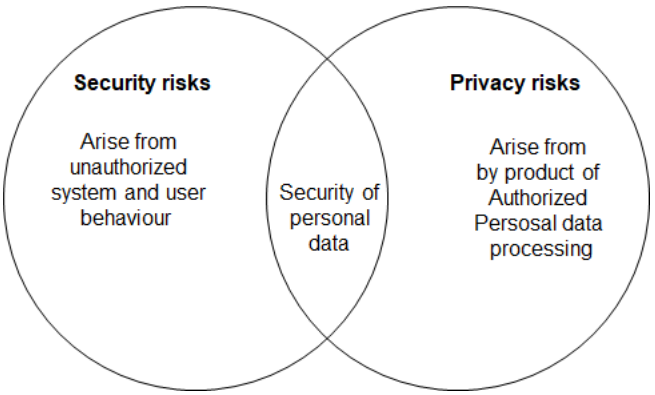
6. SECURITY AND PRIVACY ENGINEERING IN AN IOT POLICY FRAMEWORK

This chapter provides an overall analysis of security and privacy engineering in an IoT policy framework leveraging the work of the large-scale pilot program. It first summarises the main security and privacy concepts of the CREATE-IoT policy framework (D05.01). It then provides the viewpoint of standardisation on security and privacy engineering. It then provides the viewpoint of the large-scale pilots on security and privacy engineering. It finally provides an analysis integrating all viewpoints.

6.1 Input from D05.01

The below table summarizes the main security and privacy concepts of the CREATE-IoT IoT policy framework as described in D05.01. Note that this security and privacy were covered in different sections on D05.01. We suggest merging them in one section and added the term engineering to better reflect the intent of this part of the framework.

Table 21: Security and privacy concepts

Concept	Description
User-centred concerns	• A taxonomy of privacy for IoT is needed (identity, location, footprint, dynamic privacy). Trust is an essential element of dynamic privacy. • Citizen engagement needed (e.g. consultation for impact assessment). • Wealth of measures needed (e.g. serious games, crowd sourcing, voluntary certification, repository of privacy enhancing enablers).
Data protection by design	Principles are identified: • No personal data by default. • Design "As if" IoT systems will process personal data. • De-identification by default. • Data minimization by default. • Encryption by default.
Relation between security and privacy	The relationship between security and privacy (see Figure 4) is the following[50]: • Security risks arise from unauthorized system and user behaviour. Many security risks are not privacy risks, for instance the protection of an organisation confidential data. • Privacy risks arise as a by-product of unauthorized personal data processing (e.g., re-identifying a data set to an individual). • Security risks on personal data can lead to privacy risks (e.g., lack of proper consent management mechanisms, lack of security of collected personal data such as health data). 

[50] From ISO/IEC 27550 Privacy engineering for system lifecycle processes.

	Figure 4 - Relationship between security and privacy The design of privacy needs to consider: • Principles based on the ISO/IEC 29100 privacy framework[51]. • A privacy engineering methodology[52].
Security, privacy and dependability	Dependability is a well-known concept in engineering. It can be the term used in engineering to implement trust. • Properties for security are confidentiality, integrity, availability • Properties for privacy are unlinkability, transparency, intervenability • Properties for dependability include those on security and privacy. It includes further the properties of reliability, safety and maintainability.
Engineering in system life cycle processes	• Three processes are important: impact assessment, design of measures, and assurance. • Measures are organisational and technical. • The engineering objective is to reach an agreed level of protection or trust. Note that there is no agreement on how to describe this level of protection.
Organisations and roles in processes	• IoT ecosystems are complex. They can include a variety of stakeholders (authorities, IoT applications operators, IoT applications integrators, IoT suppliers (of technology, platforms). • Roles (defined in architecture standards) and collaboration schemes must be defined.
Main security domains of IoT	• A taxonomy of security domains in IoT is proposed. Such taxonomy can be of interest if it can be associated with a repository of designs and measures.
Proposed methodology	A holistic methodology is described, based on two steps: • Determination of organisation role and context (which LSP, role, data categories, relevant data life cycle phases). • Set of recommendations to follow concerning the following aspects: user/human factor, data, service, software/application, hardware, authentication, infrastructure/network).

6.2 Input from Standardisation

Table 22: Standardisation landscape on security and privacy

Security and privacy facet	
Risk management	**Situation for IoT:** There is a wealth of existing standards that can be used for risk management: • ISO 31000 covers all types of risks, ISO/IEC 27005 which covers information system security or ISO/IEC 29134 which covers privacy impact assessment. • There is agreement that impact on citizen is a priority criterion for impact analysis. For instance, ISO 21434 (cybersecurity engineering for road vehicles) focuses on four types of impact on vehicle passengers (safety, financial, operational, privacy). • Overall practice can be based on based on STRIDE and LINDDUN threats analysis, which is also described on ISO/IEC 27550 (privacy engineering). Standardisation on IoT risk management lacks guidance on the following: • No guidance is provided how architecture design activities and risk analysis activities should be integrated. Architecture decisions can have a strong impact on resulting risks. • Stakeholders in an IoT ecosystem lack guidance on how to exchange risk information. There is no agreement on a risk model with common scales for likelihood and impact assessment. There is no guidance on how acquirers and suppliers share risks. **Recommendations and opportunities for large scale projects:** Research and innovation projects have an opportunity to gain knowledge on risk management of IoT systems, in particular on the integration of architecture with risk, and on the exchange of risk information). Synergy should be put in place so that large scale projects and also other research projects

[51] Freely available at: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip
[52] Based in ISO/IEC 27550 (privacy engineering for system lifecycle processes), or the PRIPARE methodology, see http://prepareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

	ensure that knowledge gained in the risk management of security and privacy in an IoT system of systems can be contributed to standardisation.
Designing security and privacy	**Situation for IoT:** • ISO/IEC 27701 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines) published in August 2019 will be the first privacy standards with some certification scheme. It focuses on the privacy of information management systems. A proposal has been made for a new standard on organisational privacy. • ISO/IEC 27101 (guidelines to create a cybersecurity framework) provides several concepts (identify, protect, detect, respond, recover) that will help IoT stakeholders to integrate security and privacy in an IoT system design lifecycle. • A wealth of security and privacy standards is being developed on IoT. Standardisation on the design of IoT security and privacy lacks guidance on the integration of security and privacy in a system of systems: • at technical level this requires interactions with architects, • at organisational level this requires interactions with organisations in the ecosystem. **Recommendations and opportunities for large scale projects:** Research and innovation projects in the large-scale pilot program should continue to monitor the work of current standards in order to get guidance on the IoT use cases which they are developing. They should undertake a design process which involves concertation between architects and security and privacy experts at the technical level, as well as concertation between the stakeholders of the ecosystem at the organisational level. Synergy should be put in place so that large scale projects and also other research projects ensure that knowledge gained in the design of security and privacy in an IoT system of systems can be contributed to standardisation.
Assuring security and privacy	**Situation for IoT:** Two prominent security certification schemes are currently in use in ICT: • The 27001-certification scheme which focuses on the security of organisations information management systems. The recently published ISO/IEC 27701 standard can be considered as a companion standard addressing the privacy of information management systems. A similar certification scheme is likely to be established shortly. It does not address the assurance of organisations in an ecosystem. • The ISO/IEC 15408 (also known as common criteria) certification scheme which focuses on systems with security function requirements. It is very effective to ensure assurance of dedicated security subsystems, but it is very costly. Furthermore, the common criteria standard does not address the assurance of organisational measures. It does not address the assurance of complex systems today (some studies have been started) The standardisation landscape of assurance is still in the making, as we lack (1) the assurance of organisations in an ecosystem and (2) the assurance of complex systems. **Recommendations and opportunities for large scale projects:** Research and innovation projects have an opportunity to gain knowledge on assurance of security and privacy in IoT. Synergy should be put in place so that large scale projects and also other research projects ensure that knowledge gained in the risk management of security and privacy in an IoT system of systems can be contributed to standardisation.

6.3 Input from Large Scale Pilots

6.3.1 ACTIVAGE

The input in this section is taken from specific contributions, deliverables from the Activage project, as well as from the publication entitled "Next Generation Internet of Things. Distributed Intelligence and the Edge and Human Machine-to-Machine Cooperation"[53].

Table 23: ACTIVAGE feedback on security and privacy

[53] Chapter 4 of https://european-iot-pilots.eu/next-generation-internet-of-things-distributed-intelligence-at-the-edge-and-human-machine-to-machine-cooperation/

Security and privacy facet	
Risk management	The general risk analysis is characterised by the following: • It is based on the ACTIVAGE reference architecture. • An asset identification and description process is carried out for each deployment site. It includes data in the system, services, hardware, software, communication links and it can be extended to intellectual property, brand reputation, buildings, etc. • The analysis is based on the STRIDE methodology, applied to device, gateway, cloud and application. A Data protection impact assessment (DPIA) is used[54]
Designing security and privacy:	Here is ACTIVAGE analysis (done in 2018): • The nature of AHA applications requires a high level of security to keep end-to-end data integrity, confidentiality and service availability. AHA users are very concerned by these aspects. • Compliance classes should be defined, e.g. those defined by the IoT foundation framework[55]. • Security is a continuous process with integrated improvement procedure, based on the continuous evaluation of the in-place security.
Assuring security and privacy	Since security is a continuous process, continuous evaluation is needed. External inspection such as auditing is a must. Self-auditing and internal expertise are strongly enough, but by far not enough. External companies offer services to analyse the implemented security including security standards, such as ISO/IEC 27001 and 27002, the NIST Cybersecurity Framework.

6.3.2 AUTOPILOT

Table 24: AUTOPILOT feedback on security and privacy

Security and privacy facet	
Risk management	The risk management is addressed in AUTOPILOT by delivery D1.9 «Initial Specification of Security and Privacy for IoT-enhanced AD" that focuses on risk identification related to the AUTOPILOT open IoT platform for autonomous driving. The work pointed out the information assets of the system, the relevant stakeholders and the stakeholder's value for a given asset (Confidentiality, Integrity, Availability, Accountability and Authenticity), then identified the system's vulnerabilities with regard to the system interfaces, the user interfaces (including management, administration and support interfaces), the physical location of the assets and the shared communications links with other services.
Designing security and privacy:	The recommendation for designing security and privacy are provided in AUTOPILOT in deliverable D5.4 under two items: "Autonomous vehicles IoT security framework" and "Autonomous vehicles IoT privacy framework". The autonomous vehicles and IoT Security Framework issues are based on elements such as AI security mechanisms, identification, authentication, authorization, availability, confidentiality, integrity, secure analytics, network prescribed policy and secure communication, as well as security by-default, by-design and best practices. The autonomous vehicles and IoT Privacy framework is based on the human-centred concept using as a benchmark point of reference for the user centred concerns associated with privacy by addressing the basic requirements of European Data Protection Law (e.g. principle of data minimisation, privacy by design etc.).
Assuring security and privacy	AUTOPILOT has provided several recommendations for assuring security and privacy in delivery D5.4. The project has addressed the topic in a holistic manner based on the existing standards such as "Privacy framework" (ISO/IEC 29100) from the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001 and 27002 on security, ETSI ITS (e.g. ETSI TS 102 940 V1.1.1, ETSI TS 102 941, ETSI TR 102 893 V1.2.1, ETSI TS 103 097 V1.2.1), 3GPP TS 33.185, IEEE/SAE (with SCMS) standards, recommendations from ENISA (e.g. Privacy and Data Protection by

[54] Based on Guidelines on data protection impact assessment (DPIA) and determining whether procssing is « likely to result in a high risk » for the purposes of Regulation 2016/679 ; Adopted on 4 April 2017.

[55] https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

	Design and Cyber Security and Resilience of smart cars), OWASP, NIST Cybersecurity Framework and emerging needs based on the specific issues brought by autonomous vehicles and IoT technologies.

6.3.3 MONICA

Not much information available from MONICA. Deliverable D11.2 Open data management place states the following:

If data is not stored within the MONICA system, describe the mechanism for data security and backup. For sharing of sensitive data within consortium there are guidelines in chapter 4 of D10.5 (The MONICA Ethical Guidelines) that should be followed. For live pilot data it must be assessed by the Cyber Security risk management process defined in D10.11.

Table 25: MONICA feedback on security and privacy

Security and privacy facet	
Risk management	N/A.
Designing security and privacy:	N/A.
Assuring security and privacy	N/A.

6.3.4 IoF2020

In the main Farm Data is commercial data such as livestock data, soil fertility etc. and is not covered by the European legislation on personal data. That said it is still noted that there are areas where IoT monitoring may cause privacy concerns such as location and tracking of activities etc.

Table 26: IoF2020 feedback on security and privacy

Security and privacy facet	
Risk management	*"For the Security, Privacy and Trust analysis of all 19 UCs, a STRIDE analysis was realised for each individual use case. NXP provided sufficient introduction and training sessions for all trial participants to conduct a STRIDE analysis by themselves, while being supported by the WP3 teams. NXP collected the findings and started to create a security, privacy and trust scorecard for the entire project IoF2020. The goal is to provide UC owners and participating partners with technology insights throughout the 2nd, 3rd and 4th year of the project to improve their stand on security, privacy and trust. At the end of the project, NXP will once again ask partners to conduct the same STRIDE analysis to collect findings on security improvements being made in the course of the project".* D3.1 Guidelines for UC Analysis Design
Designing security and privacy	*"Consolidating the needs of the use cases enabled an overview of the main challenges, and identification of needed components. The following components have been identified, described, and are being developed in the scope of WP3:* *• IoT catalogue provides access to IoF2020 results not only to all use cases but to a wider audience. This enables a connection point between end users and solution providers, where developments and respective validations can be shared.* *• Security and privacy guidelines describe the main concerns raised by the use cases, possible analysis approaches and how to improve security by implementing the right processes and selecting suitable technologies.* *• Security enhancing enablers covers authentication and authorization management, which was one of the most common reusable components identified by the use cases and solutions for threat mitigation.* *• Context Information management describes the FIWARE context broker and NGSI, to support exchange of data, supporting unidirectional collection of data from sensors and systems, and bidirectional exchange of data among components and systems.* *• Service provision for replicability and reuse is a component that provides a solution for*

	business collaboration between an end-user and a service provider and developer. *• FMIS and reusable integration services describe the Connect API of 365FarmNet FMIS supporting creation, acquisition, exchange and visualization of data to this system.* *• Open data marketplace and configurable dashboards describes a component that supports use cases in getting the most of all the data being collected with the new IoT solutions and devices" R*ef: D3.7 UC Requirements
Assuring security and privacy	It is seen that privacy cannot fully be covered by the design of technological solutions, and they need to be dealt with in social arrangements (social norms or rules) that govern interactions between partners in the use cases. For this reason, WP7 has developed an overview over ethical issues that are encountered in the use cases and which also include issues about privacy. In the coming (last) year of IOF2020 procedures will be developed to discuss such arrangements between participants of the use cases, which future use cases will be able to reuse. Assuring security and privacy by technological means is the responsibility of WP3, being responsible for the overall architecture and IoT technology, with the areas addressed stipulated above in "Designing security and privacy". Insightful gap analysis feedback addressing this topic can be found in section 5 of D3.2 THE IOF2020 USE CASE ARCHITECTURES AND OVERVIEW OF THE RELATED IOT SYSTEMS: *"A first cyber-security analysis of most UCs has been performed using the STRIDE methodology; at the present stage, such analysis has been useful to make sure that design/specification activities also accounted for security aspects. Despite this, the STRIDE analysis is most effective when applied to complete, operational systems, also considering organizational and business-related aspects. For this reason, at the current stage of the project, for most UCs, the analysis doesn't allow proper definition and application of security-related countermeasures and must be considered high-level/incomplete, still requiring a more precise level of details to draw final conclusions.* *Nonetheless, in the last months NXP has worked at the definition of some guidelines that, starting from the STRIDE analysis reported in this document, will guide all the Use Cases in the adoption of all the necessary security measures."* *"As in the case of security-related aspects, it is difficult to plan technical/architectural aspects when the data ownership/data access aspects are not fully clarified. An additional complication exists in the definition of such aspects: as multiple parties may be involved in the creation, maintenance and exploitation of flows of data from the field, it is really difficult to accomplish the need of building a very precise picture of who operates the systems generating data, who has access to it, in which form (raw, aggregated, elaborated, etc.) and for what reason (functional reasons, maintenance purposes, audit, etc.)."*

6.3.5 SYNCHRONICITY

Table 27: SYNCHRONICITY feedback on security and privacy

Security and privacy facet	
Risk management	Risk has been managed through the reference architecture and the tools created by the project (see below)
Designing security and privacy:	High level concerns on security and privacy have been identified: a) generic statements relating to the importance of citizens privacy; b) statements that relate to transparency of the underlying processes and polices in how cities handle IoT generated data; c) statements that restrict what IoT data should be collected from an IoT infrastructure in a city; d) statements that refer to the compliance of IoT data handling with respect to laws and regulations; e) statements that refer to anonymization of personal identifiable data and its potential caveats; f) statements that outline conditions on how collected IoT data should be shared. The following high-level concerns on data management can be identified: a) statements that refer to IoT data access through open APIs;

	b) statements that refer to access to relevant historical data; c) statements that outline how IoT data should be categorized; d) statements that refer to automation of audit checks for accuracy and validity; e) statements that refer to the protection of privacy of data
Assuring security and privacy	It is important to take into account the different logical components of the SYNCHRONICITY IoT enabled Smart Cities reference architecture. The main aim of the architecture is to define a set of logical components and functionalities that can enable different cities to be actively part of IoT Smart City Digital Single Market. The composition of the different logical models can be summarized as follows: • **Context Data management**: it manages the context information coming from IoT devices and other public and private data sources, providing a context data access through a uniform interface. Context information contains status information about real world entities defined in a structured way. CDM provides functionalities to enable access to different data sources and analyse context information, e.g. for detecting events. • **IoT Management** is the module responsible to interact, through specific IoT agents, with the devices that use different standards or protocols, making them compatible and available to the SYNCHRONICITY framework; • **Data Storage Management** provides functionalities related to the data storage and access in the specific context of IoT systems and smart city platform, interacting with heterogeneous sources. • **IoT Data Marketplace** supports business interactions between data suppliers that are part of the SYNCHRONICITY ecosystem and consumers. It will implement a hub to enable digital exchange for urban data and IoT capabilities providing features in order to manage asset catalogues, orders, revenue management. These functions will support the creation of innovative business models. • **Security, Privacy and Governance**: this module covers all the security aspects related to three main pillars: data, IoT infrastructure and the platform services, which underpin the applications and services of the cities. Around these pillars, security functionalities provide crucial security properties such as confidentiality, authentication, authorization, integrity, non-repudiation, access control, etc. • **Monitoring and Platform management services**: it provides functionalities to manage platform configuration and monitor activities of the platform services. It supports specific KPI definition to evaluate the status of the platform in relation to different aspects e.g. performance, usage, reliability, quality of service etc.)

6.4 Resulting Analysis

The table below shows the resulting recommendations for security and privacy engineering in an IoT policy framework.

Table 28: Recommendations for security and privacy engineering in an IoT policy framework

Security and privacy are key cross-cutting capabilities to engineer for IoT. A IoT policy framework should include: • 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		
Risk management	Overall position	Research and innovation projects should gain knowledge on risk management of IoT systems focusing on • The impact of architecture considerations on risk management. • The problem of exchanging risk information in an ecosystem. • The use of common knowledge, such as threat models for security (e.g. STRIDE) and for privacy (e.g. LINDDUN).
	Standardisation viewpoint	Research and innovation projects should gain knowledge on risk management of IoT systems and contribute to standardisation.

	Assisted living viewpoint	Risk management includes architecture considerations, asset identification.
	Autonomous vehicle viewpoint	Risk management includes asset identification and associated stakeholder protection goals (Confidentiality, Integrity, Availability, Accountability and Authenticity, asset physical location in an architecture,
	Wearable viewpoint	N/A.
	Agrifood viewpoint	IoF2020 used the STRIDE methodology which is a threat classification model developed by Microsoft for thinking about computer security threats.
	Smart city viewpoint	N/A.
Designing security and privacy	Overall position	An integrated X-by-design approach should be taken, including citizen engagement and user-centred process, agreed principles, ecosystem issues, relying on common methods. Research and innovation projects in the large-scale pilot program should undertake a design process which involves concertation between architects and security and privacy experts at the technical level, as well as concertation between the stakeholders of the ecosystem at the organisational level
	Standardisation viewpoint	Current standards should be monitored and used for the design of security and privacy. Further guidance is lacking though, and large-scale pilots are invited to gain knowledge in their practices and contribute to standardisations.
	Assisted living viewpoint	Levels of security and privacy should be defined, which could become compliance classes.
	Autonomous vehicle viewpoint	The autonomous vehicle domain is an example where an in-depth global security and privacy approach should be taken. It was applied by Autopilot (deliverable D5.4), and the result can be used by other domains as an example.
	Wearable viewpoint	N/A.
	Agrifood viewpoint	Many issues have been identified by use cases of IOF2020 related to trust in data sharing, data access and data ownership. Privacy plays a less prominent role in considerations, as farm data do not directly reveal personal identity. Privacy plays a more indirect role. Clear rules and understandable guidance must be given to famers and other stakeholders in the agricultural chain to deal with the issues that are identified.
	Smart city viewpoint	The smart city domain is an example where an exhaustive set of policies for designing security and privacy are needed. It was applied by SYNCHRONICITY and the result can be used by other domains as an example
Assuring security and privacy	Overall position	Assurance a key aspect that has not yet be considered. The standardisation landscape of assurance is still in the making, as we lack (1) the assurance of organisations in an ecosystem and (2) the assurance of complex systems. Assurance approaches must also leverage architecture commonalities.
	Standardisation viewpoint	Research and innovation projects have an opportunity to gain knowledge on assurance of security and privacy in IoT. Synergy should be put in place so that large scale projects and also other research projects ensure that knowledge gained in the risk management of security and privacy in an IoT system of systems can be contributed to standardisation.
	Assisted living viewpoint	Since security is a continuous process, continuous evaluation is needed. External inspection such as auditing is a must.
	Autonomous vehicle viewpoint	The assurance security and privacy for autonomous vehicles is an important issue that is still not solved yet. The views of the security community and the vehicle industry community still have to be aligned.
	Wearable viewpoint	N/A.

	Agrifood viewpoint	Security and privacy remain important topics of consideration. However, it may not always be clear when protection is needed, as farmers may have a different understanding of what data are 'private' and deserve to be protected than other stakeholders. The meaning of concepts such as privacy is shifting during the digitalisation process and needs to stabilize before clear demands for protection can be made.
	Smart city viewpoint	The assurance of security and privacy for smart cities must take into account the various logical components of a smart city reference architecture (context data management, IoT management, data storage management, IoT data marketplace; security/privacy/governance, monitoring and platform management services)

7. CONCLUSIONS

This section is a synthesis of sections 4.4 (Resulting Analysis), 5.4 (Resulting Analysis), and 6.4 (Resulting Analysis)

7.1 What we Learned

The work carried out by CREATE-IoT in supporting the large scale pilots confirmed the relevance of using (and contributing to) an IoT policy framework with three pillars:

- 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:
  - 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, connectability, resilience, availability, dependability, privacy. confirmed the need to
- Organisation engagement is a key prerequisite for successful IoT. A IoT policy framework should include:
  - Measures for ethics engagement.
  - Measures for standardisation engagement.
  - Measures for legislation engagement.
  - Measures for contracts engagement.
- Security and privacy are key cross-cutting capabilities to engineer for IoT. A IoT policy framework should include:
  - 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

7.2 Conclusions and Recommendations

Conclusions could be reached, and recommendations identified further to the common work with the large-scale pilots: ACTIVAGE, AUTOPILOT, MONICA, IoT2020, and SYNCHRONICITY. They have led to the following policy commonalities that could be of horizontal relevance for all verticals:

Trust includes a socio-economic perspective, a business perspective, and a technical perspective. Concerning the socio-economic perspective, policies should include measures to enable economic progress associated with social progress. Further, a trustworthy IoT environment must therefore cover business operations associated with social processes. Concerning the business perspective, policies should include measure integrating factors relevant for trust, such as reputation, taking into account user's perception and the social environment. Concerning the technical perspective, policies should leverage an agreed architecture description and terminology that can be based on current work in the IoT community. Deliverable D06.02 (Recommendations for commonalities and interoperability profiles of IoT platforms) suggests a 3D model based on layers, cross-cutting functions, and properties. Further, these policies will

have to identify the elements to which trust should be achieved (e.g. device trust, system trust, data trust).

Organization engagement includes ethics, standards, legislation and contracts. Concerning ethics, practice for business ethics and corporate social responsibility should be carried out as they are highly relevant for the IoT environment. Concerning standards, policies should include measures to foster the contribution and adoption of standards related to trust: assessment, measures, assurance. Concerning legislation, policies should include measures to monitor the evolution of legislation related to IoT on security and privacy. Concerning contracts, the advent of IoT ecosystems will require agreement frameworks. Research and innovation projects and large-scale pilots should monitor and possibly contribute to contractual practice.

Security and privacy engineering includes risk management, design of security and privacy, and assurance of security and privacy. Concerning risk management, research and innovation projects should gain knowledge on risk management of IoT systems focusing on (1) the impact of architecture considerations on risk management, (2) the problem of exchanging risk information in an ecosystem and (3) the use of common knowledge, such as threat models for security (e.g. STRIDE) and for privacy (e.g. LINDDUN). Concerning design of security and privacy, an integrated X-by-design approach should be taken, including citizen engagement and user-centred process, agreed principles, ecosystem issues, relying on common methods. Further research and innovation projects in the large-scale pilot program should undertake a design process which involves concertation between architects and security and privacy experts at the technical level, as well as concertation between the stakeholders of the ecosystem at the organisational level. Concerning assurance of security and privacy, research and innovation projects have an opportunity to gain knowledge on assurance of security and privacy in IoT. Synergy should be put in place so that large scale projects and also other research projects ensure that knowledge gained in the risk management of security and privacy in an IoT system of systems can be contributed to standardisation.

7.3 Going Further

With D05.01, D05.02, D05.06, CREATE-IoT has provided contributions on the IoT policy framework and its evaluation and on the IoT legal framework. These documents provide a synthesis of knowledge and experience collectively gained in the first wave of large-scale pilots. We are in the middle of the road. These documents should be an input to the new wave of pilots and the content should be further enhanced.

ANNEX: UPDATED IOT POLICY FRAMEWORK

This section is an update of D05.01. The reader who is already familiar with D05.01 can skip this section. However, there are few updates which are highlighted in yellow.

A.1 Introduction

There are multiple definitions available for the Internet of Things (IoT); the European research community, for instance, defines IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"[56], while at the same time, the International Telecommunication Union and, more specifically, the Standardization Sector (ITU-T) has defined IoT as , "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[57]. Taking both these definitions into account, it becomes apparent that through identification, data capture, processing and communication capabilities, IoT maximises the use of physical objects (things) to offer services for a wide variety of applications, whilst at the same time it is important to ensure the fundamental rights for individuals and society at large. It therefore is argued that IoT, in its widest sense, forms a materialization of a vision which is based on the exploitation of knowledge thus creating a series of technological and societal implications which calls for responsible interventions.

In the last few years, the IoT has gained widespread detrimental attention due to the extensive occurrences of IoT security related incidents affecting devices that are commonly used on a daily basis; fitness watches, thermostats, printers, refrigerators. These devices were brought to the centre of the discussions taking place worldwide, as examples that were poorly secured were targeted by malicious actors for various malign purposes. More specifically, due to the fact that IoT devices are sensing, actuating and processing units (in the future including intelligent, cognitive devices, autonomous systems and robotic things) connected to a network, and have operating systems with the ability to perform quite complex computational operations, they create opportunities for exploitation by malicious actors. Those malicious actors may take advantage of the absence of sufficient security measures in place, as certain IoT devices, for instance, do not require passwords at all, while others are sold to consumers with default passwords that many users do not change.

Nevertheless, the development of IoT applications and smart devices at the edge of the network is increasing and the rapid prototyping and "rush-to-market" strategies are creating the right circumstances for increasing the volume of possible incidents.

It is the value of using IoT devices and applications per se that increases the motivation of malicious actors to act. The extensive dependence on undependability of IoT devices entails a series of consequences that may create an unwelcome and growing impact on everyday life of individuals, on economies as well as on national security.

---

[56] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

[57] International Telecommunication Union – ITU-T Y.2060 - (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of things

In response to the increasingly growing risks and associated impacts, regulators across the globe have started taking action in order to address specifically the IoT ecosystem. For example, in August 2017, a bill i.e. the Internet of Things (IoT) Cybersecurity Improvement Act of 2017 was introduced in the Senate of the United States[58] to provide minimum cybersecurity operational standards for internet-connected devices purchased by Federal agencies. The bill promises to incentivise malicious actors to expose vulnerabilities in flawed devices and prohibit vendors from selling devices with unchangeable passwords, or with known vulnerabilities, while at the same time providing legal ground to encourage vendors to ensure that their internet-connected equipment is patchable i.e. able to be protected retrospectively through updates in the firmware and software. The proposed regulatory instrument is largely consistent with an ongoing multi-stakeholder effort led by the National Telecommunications and Information Administration (NTIA) aimed at developing voluntary security standards for Internet-connected devices.

Key elements of the proposed legislation relate to the setting of IoT security standards building on vendor compliance and commitment to provide, amongst others, for IoT devices to be patchable and that IoT devices do not contain hard-coded passwords. However, this particular instrument does not provide for any direct enforcement mechanisms for vendors of IoT devices aside from the threat of disqualification from federal contracting opportunities. It is proposed that these requirements are, however, limited to contractors participating in the federal procurement market, which means that the bill only applies to vendors that sell IoT devices to the government and that other consumer devices are exempted from such requirements. A revised version of the bill was introduced in the Senate in March 2019 with the same scope i.e. government IT procurement. Unlike the 2017 version, the 2019 bill requires NIST to develop recommendations that cover identity management, patching, secure development and the like. Given that IoT devices have gained a lot of traction in the last few years, it is expected that the revised bill will fructify into law.

In the light of the associated developments, creating an IoT Policy Framework that would address trust, engagement, privacy and security in an appropriate manner for individuals and society is essential for the sustainability and trustworthiness of IoT ecosystems within EU and beyond.

Building on the existing definitions and approaches adopted within the EU and beyond[59],[60],[61],[62] highlighting, also, privacy and trust among other issues relating to IoT from an ethical point of view[63], this section builds a policy framework appropriate for the IoT environment[64]. It produces a synthesis of the related principles, functions, definitions, requirements and practices identified, within the IoT European Large-Scale Pilots Programme. The IoT Policy Framework to be addressed under this analysis is composed of distinct components, namely, the trust framework, the engagement framework, the security and privacy engineering framework prioritized and structured in way that further reveals the underlying human centred approach.

[58] Note that the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'' published in September 2017 explicitly addresses the risks associated to connected devices.

[59] Developing a Framework to Improve Critical Infrastructure Cybersecurity, NIST 2013.

[60] O. Vermesan and J. Bacquet (Eds.). Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017

[61] Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016, U.S. Department of Homeland Security.

[62] An in-depth discussion of the existing approaches falls outside the aims of the present deliverable; a more elaborated discussion, though, will be provided –to a certain extent- under the final deliverable due in December 2019.

[63] Europe's policy options for a dynamic and trustworthy development of the Internet of Things, Final Report (D7) 2013, Prepared for the European Commission, DG Communications Networks, Content and Technology (CONNECT).

[64] Note that there are multiple definitions on the notion of framework per se. For instance, the framework is defined as "a *basic structure underlying* secure human centric IoT systems'' or as "*a system of rules, ideas, or beliefs that is used to plan or decide something".* See, also, https://en.oxforddictionaries.com/definition/framework and http://dictionary.cambridge.org/dictionary/english/framework

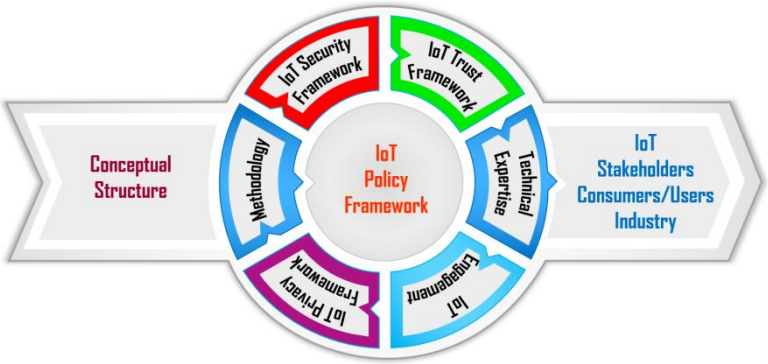


Figure 5: IoT Policy framework aims and target group

In particular, the IoT Trust Framework provides an underlying structure and a set of principles that manifest trustworthiness, dependability and privacy for IoT solutions in an integrated manner. This framework integrates the concepts of availability, reliability, safety, security resilience, privacy and sustainability best practices, embracing "privacy and security by design" as a model for an implementable IoT code of conduct and engagement.

In view of the ultimately aim of a human centric approach, a key pillar of the present deliverable document, the discussion expands on the creation of an IoT Engagement Framework producing the need for stakeholders' engagement to ethics, rules, guidelines and standards for an effective IoT Policy Framework that would safeguard a sustainable and safe IoT environment in the long run. To this end, the analysis points to emerging regulatory and contractual relationships relevant for the Large-Scale Pilots (LSPs) and highlights the challenges for engagement and compliance at this time of significant changes in the European regulatory arena. Note that stakeholders' engagement in relevant soft law instruments (e.g. best practices, standards and guidelines), is what underlies the aforementioned bill currently discussed in the US, while, also, being reflected in European instruments including the General Data Protection Regulation (GDPR) and the Regulation on the Free Flow of Non-Personal Data[65] that both strengthen the role of soft regulation.

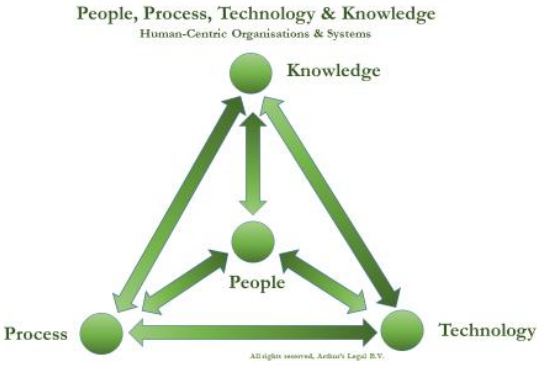


Figure 6: IoT consisting of People, Process, Technology and Knowledge

The IoT Security and Privacy Engineering Framework, starting from the user centred concerns and considering GDPR, covers key aspects of the European Data Protection law, addressing, more specifically, the principles of data protection by design and data minimization. A principle based approach with respect to privacy would give stakeholders room and freedom, with respect to the appropriate means to employ, in order to achieve the level of protection aspired to by the Regulator; for example, commitment to standards may be an appropriate behaviour for

[65]European Commission COM(2017) 495 final 2017/0228 (COD), Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 2017, online at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF

companies to demonstrate compliance with the data protection rules in the context of Business to Business relationships, while the endorsement of best practices could be an appropriate means to build individuals trust in the context of the Business to Consumers relationships.

The IoT Security and Privacy Engineering Framework is further based upon a methodology of evidence gathering to ensure the user/customer industry derive suitable IoT security mechanisms and practices which are appropriate within the IoT applications domain and solutions in various sectors. It, also, paves the way forward by indicating best practices and choices in design, features, implementation, testing, configuration and maintenance as well as a dedicated methodology for facilitating compliance by design within the changing regulatory landscape. The particular traits of the concepts to be discussed, namely, trust, security, privacy, engagement, are reflected in the structure of the entire annex, as well as in the structure of the dedicated sections. More specifically, and in the context of the human centred approach adopted, the more theoretical discussion on the trust framework precedes the discussion on privacy and security. Similarly, the discussion on the privacy framework has as a starting point the user centric concerns linking to privacy.

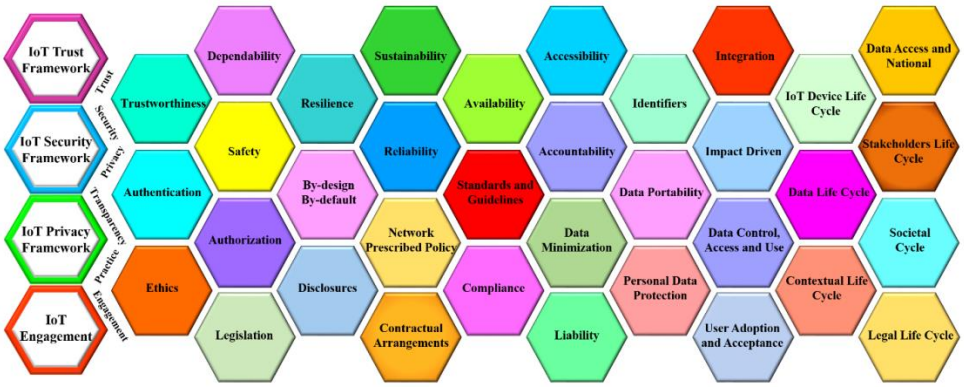


Figure 7: Constitutive elements of the IoT Policy framework

Figure 7 captures the entire set of items that emerged so far in the discussions, as well as from the literature review of the existing frameworks, while providing an illustration of the multidisciplinary expertise of consortium partners.

A.2 The IoT Trust Framework

This section will first give an overview of the various interpretations assigned to trust and the meaning it obtains under the different perspective examined (namely, the socio-economical and the business perspective). Second, it identifies the trust component and, finally, it proposes a trust framework.

Figure 8: IoT Trust Framework

Overall, the IoT Trust Framework provides collective principles and underlying structure that exhibit the trustworthiness, dependability and privacy for IoT solutions into an integrated manner. The framework integrates the concepts of availability, reliability, safety, security

resilience, privacy and sustainability best practices, embracing "privacy and security by design" as a model for an implementable IoT code of conduct and engagement.

A.2.1 Trust: A Chameleon Concept

The notion of trust constitutes a highly complex concept used across disciplines and assigned with various interpretations. The societal, human, user, technological, information, and knowledge -centred trust perspective, as well as the interdisciplinary discourse of social and economic life have generated a debate surrounding the concept of trust. This debate has emerged across various scientific and research domains, such as the social sciences[66], philosophy[67], political science[68], social anthropology[69], transaction cost economics[70], art and design[71],[72], sociology[73], economic sociology[74], computer science[75], the IoT[76] and cloud computing[77].

No definition of trust is complete; what is more, the existing definitions differ both between and within disciplines. The diversity of notions and concepts reveals a 'degree of confusion and ambiguity that plagues current definitions of trust'[78]. The range of definitions creates challenges in working with formalised models of computational trust for assisting the decision-making of human and artificial entities (sensor/actuator nodes, intelligent/cognitive instruments, robotic devices, etc.). Since the digital transformation of society is moving the issue into the mainstream of economic and technological disruption, socio-economic and technological notions of trust both need to be addressed holistically.

The trust concept is used in various contexts and with different meanings. Although its importance is widely recognised, trust is a complex notion about which no definitive consensus exists in the scientific literature. A primary problem with many approaches towards the definition of trust is that they do not lend themselves to the establishment of metrics and evaluation methodologies. Moreover, the satisfaction of trust requirements relates strictly to identity management and access control issues.

---

[66] R. Swedberg, "Economic sociology: past and present", Current Sociology, Vol 35 No 1: 1-221, 1987, pp. 131.

[67] B., Williams, "Formal structures and social reality" in D. Gambetta (ed) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell: 1988, pp. 3-13.

[68] J. Dunn, "Trust and political agency" in D. Gambetta (ed) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell: 1988, pp. 73-93.

[69] K., Hart, 1988, "Kinship, contract, and trust: the economic organization of migrants in an African city slum" in D. Gambetta (ed.) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell.

[70] O. Williamson, "Calculativeness, trust, and economic organization", Journal of Law and Economics, Vol 36 No 2, 1993, pp. 453-486

[71]Digital transformation of industry, Roland Berger Report, 2015, online at: https://www.rolandberger.com/publications/publication_pdf/roland_berger_digital_transformation_of_industry_20150315.pdf

[72] D. Hemment, J. Bletcher, and S. Coulson, Art, creativity and civic participation in IoT and Smart City innovation through 'Open Prototyping'. In Proceedings of the Creativity World Forum 2017. Aarhus, Denmark. November 1-2, 2017.

[73] N. Luhmann, 1988, "Familiarity, confidence, trust, problems and alternatives", in D. Gambetta (ed), Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell

[74] Granovetter, 1985, "Economic action and social structure: the problem of embeddedness, American Journal of Sociology, Vol 91: 481-510.

[75] J. Sabater and C. Sierra, "Review on computational trust and reputation models," Artif. Intell. Rev., vol. 24, pp. 33–60, September 2005

[76] F. Bao and I. Chen, "Trust management for the internet of things and its application to service composition," in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, USA, June 25-28, 2012. IEEE Computer Society, 2012, pp. 1–6, online at: http://dx.doi.org/10.1109/WoWMoM.2012.6263792.

[77] K. M. Khan and Q. M. Malluhi, "Establishing trust in cloud computing," IT Professional, vol. 12, no. 5, pp. 20–27, 2010.

[78] C., Castelfranchi and R., Falcone, Trust Theory: A Socio-Cognitive and Computational Model. Wiley Series in Agent Technology. John Wiley & Sons Ltd., Chichester, 2010.

Online trust is a customer's willingness. It enables accepting an online transaction according to their positive and negative expectations regarding future online shopping behaviour[79]. Trust is the willingness of a party to be vulnerable to the action of another party, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party[80]. There is an attitude of confident expectation that one's vulnerabilities will not be exploited in an online situation of risk[81]. The trusting agent has a belief in the trusted agent's willingness and capability to deliver a quality of service in a given context and in a given timeslot[82].

According to Dauber[83], trust can be decomposed in device trust, entity trust and data trust. Device trust is a challenge, since *a priori* trust in devices cannot always be established (e.g. due to high dynamics and cross main relations). Hence, approaches such as trusted computing[84] and computational trust[85] are required to establish device trust. Every entity may assess trust in a device differently.

IoT architectures have to deal with its different perspectives of trust entity, while trust in the IoT applications and deployments refer to the expected behaviour of the participants, such as persons or services.

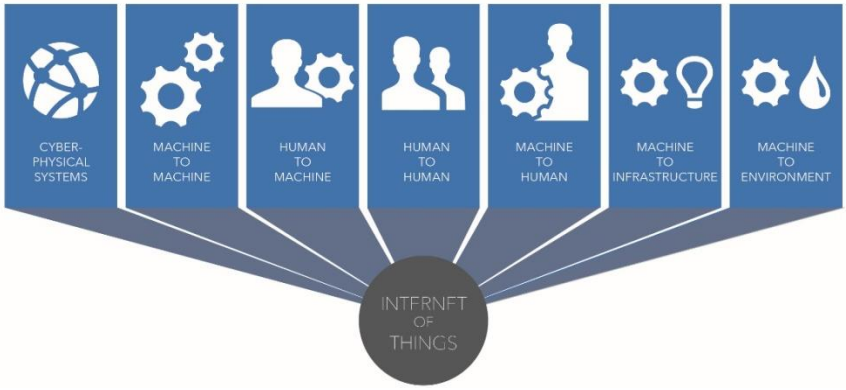


Figure 9: IoT interactions

Device trust can be established via trusted computing and mapping different approaches to device trust is claimed to be more challenging and still in the experimental phase. The authors argue that data trust occurs in a twofold manner in the IoT. First, trusted data may be derived from untrusted sources by aggregation. Second, IoT services themselves can create data for which trust assessment is required.

As far as IoT is concerned, the complexity of the interactions involved calls for an approach to trust at a high level, end-to-end, at each architectural layer and at the interfaces, M2M (Machine-

[79] K. Kimery and M. McCard, "Third-party assurances: Mapping the road to trust in e-retailing," Journal of Information Technology Theory and Application, vol. 4, no. 2, pp. 63-82, 2002.

[80] R. Mayer, J. Davis and F. Schoorman, "An integrative model of organizational trust," The Academy of Management Review, vol. 20, no. 3, pp. 709-734, 1995.

[81] C. Corritore, B. Kracher and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," Int.J. Human-Computer Studies, vol. 58, no. 6, pp. 737-758, 2003

[82] E. Chang, T. Dillon and F. Hussain, "Trust and reputation relationships in service-oriented environments," ICITA 2005. Third International Conference on Information Technology and Applications, vol. 1, pp. 4-14, 2005.

[83] J. Daubert, A. Wiesmaier and P. Kikiras, "A review on privacy and trust in IoT," in In IoT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015, London, 2015

[84] I. Alexander and W. Sean, "Protecting client privacy with trusted computing at the ser," in IEEE Security and Privacy, 2005

[85] J. Audun, I. Roslan an B Colin, "A survey of trust and reputation systems for online service provision," Decision Support Systems, Vol. 43, No. 2, pp. 618-644, 2007.

to-Machine), H2M (Human-to-Machine), H2H (Human-to-Human), M2H (Machine-to-Human), M2I (Machine-to-Infrastructure), and M2E (Machine-to-Environment).

In the IoT ecosystem the complexity of interactions requires addressing the trust at the high-level, end-to-end, at each architectural layer and at the interfaces, M2M (Machine-to-Machine), H2M (Human-to-Machine), H2H (Human-to-Human), M2H (Machine-to-Human), M2I (Machine-to-Infrastructure), and M2E (Machine-to-Environment).

A.2.2 Social-Economical Perspective of Trust

Trust is recognised as an important element in negotiations and transactions in the economic and political arena. It is acknowledged that, 'the advantage to mankind of being able to trust one another penetrates into every crevice and cranny of human life'[86].

The reason for analysing trust from an economic perspective stems from the recent popularisation of the argument that trust enhances economic efficiency under certain conditions. This hypothesis can be traced back to Mill[87], who emphasises that trust can reduce the transaction costs of enforcing honest behaviour and those situations in which an absence of trust causes inefficiency are of equal, if not more, concern.

There is a distinction between the attribute of trust and the behaviour of trust[88]. Different types of trust are identified according to their role: commercial, problem solving, informational, knowledge or identity[89], based on the area of use: behavioural, business or technology[90] and from different perspectives on trust: individual, societal or relationship[91].

A method[92] was proposed to explore the different meanings of trust and strategies that can be used to determine whether something is trustworthy and the proposed model for trust that takes people, devices and their connections into consideration. This model uses *a priori* and *a posteriori* trust to provide an indication of how much a user can trust or distrust the information provided by things. This trust indicator can inform users' decisions on whether to use a device or service or not.
Virtually every commercial transaction has an element of trust within itself, as does any transaction conducted over a period of time. It can be plausibly argued that much of the economic backwardness in the world can be explained by a lack of mutual confidence. The absence of trust may be particularly prevalent in numerous developing and transition economics in which economic transactions are viewed as exploitative, rather than mutually beneficial.

A.2.3 Business Perspective of Trust

Trust in IoT is an indispensable prerequisite for the growth of IoT business. This growth of IOT business is further subject to a series of adoption factors relevant for trust. In particular, as far as providers are concerned, their reputation is of key importance for the response of IoT users. Similarly, trust entails users' psychological feeling about the adoption. In a broader scale, trust from a business perspective involves user's perceptions as shaped by the social environment.

[86] J.S., Mill, Principles of Political Economy, London: Longmans, 1891, pp. 68.
[87] ibid.
[88] P. Pettit, "The Cunning of Trust", Philosophy and Public Affairs 24, 1995, pp. 202-225
[89] B. Misztal, Trust in Modern Societies, Polity Press, Cambridge MA, 1996.
[90] A. McCullagh, "E-commerce: A Matter of Trust", in Proceedings of the 1998 Information Industry Outlook Conference, 1998.
[91] A. Kini, and J. Choobineh, "Trust in Electronic Commerce: Definition and Theoretical Considerations", in W. Blanning, and D. King, (eds.), Proceedings of the 31 Annual Hawaii Conference on System Sciences, volume IV, IEEE Computer Society, 1998.
[92] W. Leister and T. Schulz, "Ideas for a Trust Indicator in the Internet of Things," in Th First International Conference on Smart Systems, Devices and Technologies, 2012

Furthermore, on a more concrete basis, trust in the business context, primarily, links to the product's characteristics and the risks occurring through its mere use.

Figure 10: IoT Trust balance

Strategies, products and services to enhance trust can be evaluated along different dimensions, while different implications on trust and privacy address the *whom (participant element), where (dimension, area, boundaries), when (publication, release), who (investor, stakeholder paying) and how much (cost).*

Understanding the different dimensions is important in developing rules, guidelines and policies for evaluating, monitoring, comparing and developing different approaches and products to deal with specific trust-enhancement goals.

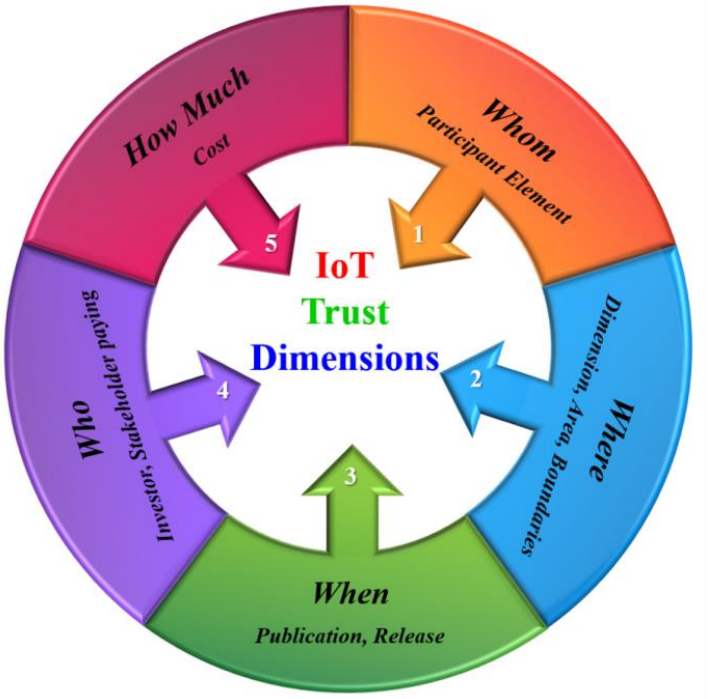


Figure 11: IoT Trust dimensions

The 'whom' is represented by the participant element (human, thing, software agent) covered by a particular approach to trust enhancement. 'Where' is represented by the area or dimension that refers to the boundaries for the trust-enhancing mechanisms. 'When' is addressed by the publication of the legislation or other trust- enhancing approach to be made available or released. 'Who' is represented by the one to be charged for the trust-enhancing product or service and 'how much' is represented by the cost to be charged to obtain a trust-enhancing product or service, such as certification.

A.2.4 Trust Components

Designing for trust requires the identification of elements and mechanisms of trust that can be embedded in a system. Defining trust as the intersection of privacy, security and reliability can enable or simplify the identification of trust as embedded in a technical design, such as in IoT systems. Since trust assumptions are built in when data collection is enabled or coordination is made feasible, trust can be built into systems, even those without security.

Trust is an element with multiple dimensions combining, for example, privacy, security reliability, availability, and integrity with human and machine behaviour. In this context, there is a need for greater understanding of how individuals interact with machines and how machines/things interact with other machines/things with respect to the extension of trust.

Trust is a function of privacy, while security reliability, availability, and integrity are operational elements based on risks, rather than user perception of risk, and focused on the existence of risk (Boolean), rather than quantifying the risk (deterministic or stochastic). Privacy is a measure of the tendency to share information (tendency is based on the risk of secondary use of information rather than a psychological sensitivity to information exposure). It is the right to act without observations and it applies to people. The connection between privacy and autonomous things is an evolving theme.

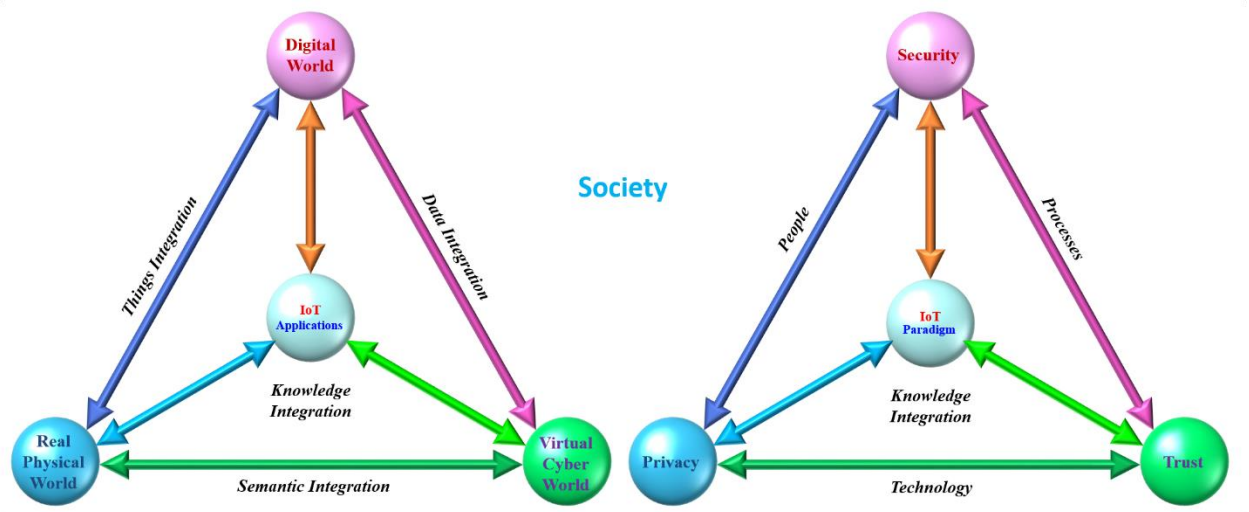


Figure 12: Trust as part of the IoT physical, digital, virtual and cyber convergence

Although confidentiality is an element of both security and privacy, this commonality does not make them the same. Confidentiality allows a person/thing to communicate to another without eavesdroppers and, in general, the control of information enabled by security does not imply privacy. Security enables the control of digital information, while social, organisational and technological (i.e. autonomous, cognitive, artificial intelligence systems) forces determine who exercises the power of that control. Privacy requires that a person/thing be able to control information about his-/her-/itself. Security provides the ability to generate privacy in a specific case (as with the confidentiality of communication), or the capacity for cryptography, which is the art of hiding information. Security can be considered to provide anonymity when the information that is hidden is identifying information. Anonymity is a technical guarantee of privacy.

Trust implies secure endpoints and it requires that security mechanisms do not affect survivability. The Internet Protocol is distributed and exhibits graceful degradation, which means that any computer/thing/device can connect to a network without altering the access of others. The loss of one computer/thing/device should not affect those who are not using its services. The ability of any network, the Internet or an intranet, to degrade gracefully rather than suffering catastrophic failure is a critical component in survivability. Both security systems and the lack of

security systems enable denial of service attacks. Security systems that are computationally intensive or intolerant of user input make it more likely for a user to experience a lack of reliability.

The trust mechanisms in today's IoT are based on all-or-nothing trust relationships. A network resource request is not trusted before authentication and after authentication, it is granted the full credentials of the corresponding user. Executable content from within a protected network is completely trusted, but content from outside the firewall is strictly disallowed. Once established, a network connection has equal priority with all other network connections on the system. These all-or-nothing trust relationships fail to match the expectations of users and the needs of next generation network applications. Since users undermine simplified trust models to meet their own complex resource-sharing needs, this mismatch promotes security breaches among users.

Although the firewall model of trust is very simple for use in distinguishing secure sources of executable content, there is a need for distributed trust modes that allow distinctions to be made in the trustworthiness of network entities. Security in today's Internet is focused on a centralised model where strong security requires a firewall. The firewall is a barrier, but once it has been compromised, the entire network that it protects is compromised, making the firewall a single point of failure. The tunnelling example demonstrates how this centralised approach can allow a single breach of security to compromise the security of an entire protected IoT network.

Figure 13: IoT Trust components

Design for trust requires enumerating the social assumptions and examining how those assumptions can function to put some user of the system at risk. To understand and design trust systems requires acknowledgement of the social, human and autonomous/cognitive elements.

From an information and communication technology perspective, trust actually refers to trust measurement capabilities and –similarly- privacy actually refers data protection capabilities. This definition mirrors trust assessment approaches, such as recommendation and reputation systems, which calculate the trustworthiness of one subject to match it against the need for trust of another subject.

A.2.5 IoT Trust Framework

The IoT is bridging the virtual, digital, physical worlds and mobile networks need to scale to match the demands of billions of things, while the processing capabilities require addressing the information provided by the "digital shadow" of these real things. This need focusing on the developments in the virtual world and the physical world for solving the challenges of IoT applications. In the virtual world, network virtualization, software-defined hardware/networks, device management platforms, edge computing and data processing/analytics are developing fast and urgency to be endeavoured as enabling technologies for IoT. Connecting the virtual, digital, physical worlds generates knowledge through IoT applications and platforms, while addressing security, privacy and trust issues across these dimensions.

Smart IoT applications modify the way people interact with the intelligent spaces (called also cyber-spaces), from how remotely control appliances at home to how the care for patients or elderly persons is perform. The massive deployment of IoT devices represents a tremendous economic impact and at the same time offers multiple opportunities. IoT's potential is underexploited, the physical and intelligent are largely disconnected, requiring a lot of manual effort to find, integrate, and use information in a meaningful way. IoT and its advances in intelligent spaces advances can be categorised along with the key technologies at the core of the Internet.

Ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting the concept of trusted IoT based on the features and security provided of the devices at various levels of the digital value chain.

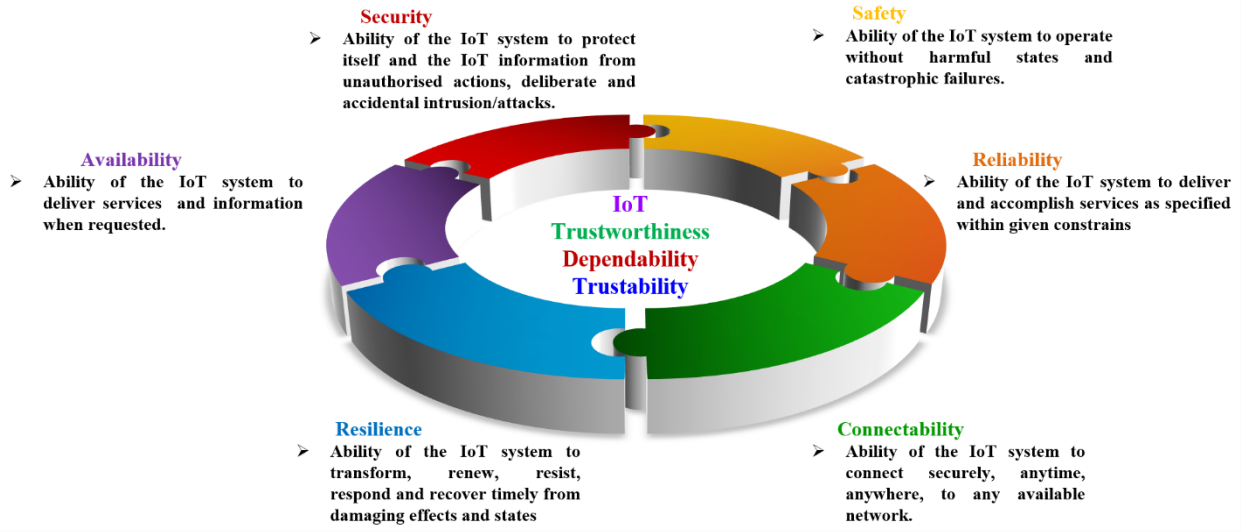


Figure 14: IoT complex interlinked concepts of trustworthiness, dependability and trustability

Security needs to be designed into IoT solutions from the concept phase and integrated at the hardware level, the firmware level, the software level and the service level. IoT applications need to embed mechanisms to continuously monitor security and stay ahead of the threats posed by interactions with other IoT applications and environments. Trust is based on the ability to

maintain the security of the IoT system and the ability to protect application/customer information, as well as being able to respond to unintended security or privacy breaches. In the IoT ecosystem, it is important to drive security, privacy, data protection and trust across the whole IoT ecosystem and no company can "do it alone" in the IoT space; success will require organizations to partner, value chains to be created and ecosystems to flourish. Yet, as IoT users start to bring more players, service providers and third-party suppliers into their value chain, tech firms and IoT solutions providers will face increasing pressure to demonstrate their security capabilities[93].

A layered IoT architecture is proposed for a trust management control mechanism[94]. The IoT infrastructure is decomposed into three layers: sensor, core and application. Each layer is controlled by a specific trust management under the following purposes: self-organisation, routing and multi-service, respectively. The final decision-making is executed by the service requester (i.e. the user) according to the collected trust information and the requester policy. A formal semantics-based and fuzzy set theory are used to realise the trust mechanism.

The distinction between trust and the related concepts of trustworthiness, confidence and the act of entrusting something to someone are extremely important. Uncertainty and vulnerability are two of the core elements in trust relations. In addressing issues of trust, actors select strategies that reduce uncertainty or decrease vulnerability, depending on the particular context in which the issues emerge. Mechanisms for reducing vulnerability in the face of increased contact with unknown things include enforceable contracts, insurance schemes, etc. The characteristics of different types of trust relations include faith, confidence, legal trust and trust/distrust.

Since it is a sign of a more usual quality known to be correlated with trustworthiness (for example, same group, class, family, or same source), identity ‘signals’ trustworthiness in many cases.

The works of Bao and Chen[95],[96] focus on trust level assessment of IoT entities. These authors assume that most smart objects are human-carried or human-related devices, so they are frequently exposed to public areas and communicate through wireless and are consequently vulnerable to malicious attacks. Smart objects have heterogeneous features and need to work together cooperatively. Since users are friends among themselves (i.e. friendship), users own the devices (i.e. ownership) and the devices belong to some communities (i.e. community), the social relationships considered include friendship, ownership and community. Malicious nodes directed towards breaking the basic functionality of IoT through trust related attacks include self-promoting and bad- and good-mouthing. The trust management protocol for IoT proposed by Bao and Chen is distributed, encounter- and activity-based: two nodes that come in contact with each other or are involved in a mutual interaction can rate each other directly and exchange trust evaluations about the other nodes; therefore, they perform an indirect rating, which seems like a recommendation. The reference parameters to trust evaluation include honesty, cooperativeness and community-interest. Such a dynamic trust management protocol is capable of adaptively adjusting the best trust parameter setting in response to dynamically changing environments to maximise application performance.

---

[93] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., “Internet of Things Strategic Research Agenda”, Chapter 2 in Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

[94] L. Gu, J. Wang, B.B. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156].

[95] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT "12, USA, San Jose, 2012, pp. 1–6.

[96] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.

A.3 The IoT Engagement Framework

This section discusses the IoT Engagement[97] Framework, a constitutive component of the overarching IoT Policy Framework. In particular, first, it gives an overview of the related engagement mechanisms; second, it depicts the regulatory and contractual relationships and, third, it gives an overview of the challenges for compliance – and engagement – at this moment of change of the European regulatory scene. In the context of the present analysis engagement is defined as follows: "engagement refers to commitment and endorsement of norms and values through concrete practices".

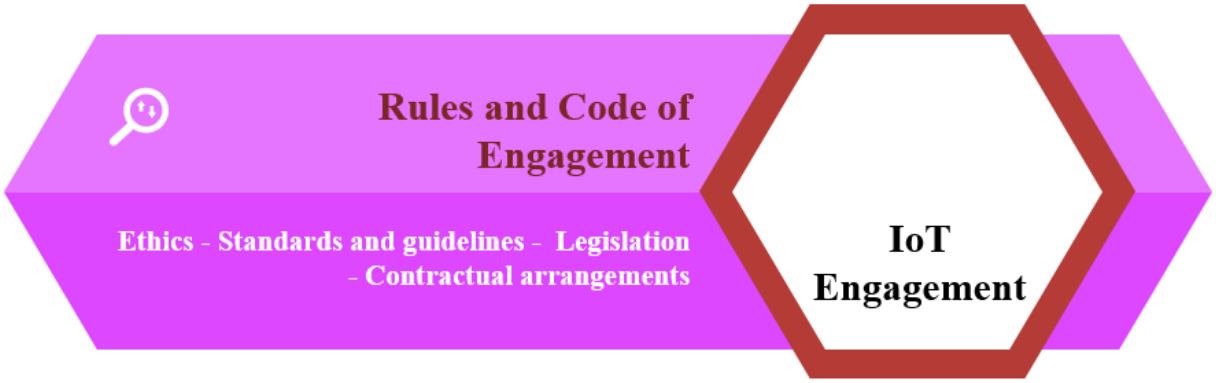


Figure 15: IoT engagement framework[98]

A.3.1 The Engagement Mechanisms

The section gives an overview of the benchmark points of reference for the entire spectrum of IoT stakeholders ensuring engagement in an appropriate manner for the IoT environment. The figure below captures the steppingstones of engagement, meaning, Ethics, Standards and Guidelines, Legislation and Contractual Arrangements. It has been noted that much ink has been spilt in by scholars dealing with the above-mentioned concepts – the discussion below expands on them. A more in-depth discussion – from a legal standpoint – is elaborated under "D05.05 Legal IoT Framework" and "D05.06 Legal IoT Framework Evaluation & Final Legal IoT Framework".

As far as the notion of Ethics is concerned, this is assigned with fundamental importance, as engagement to ethics is what – in essence – underlies engagement to the rest of the items identified. The notion of Ethics per se is vast including a series of different kinds of Ethics[99] identified. The most relevant categories of Ethics for the IoT Environment are the "Business Ethics" and "Digital Ethics."

Business Ethics and, more specifically, Corporate Social Responsibility are highly relevant for the IoT environment. Corporate Social Responsibility is, in general, understood as actions performed by businesses that i) are not dictated by law and ii) aim at benefiting entities other than a business corporation. Business Ethics, in this sense, are highly relevant for IoT due to its' impact on society at large.

Furthermore, digital ethics are found at the heart of the discussions at EU level concerning data protection matters. The European Data Protection Supervisor urges "the EU and also those responsible internationally, to promote an ethical dimension in future technologies to retain the

[97] The annex includes an initial version of Code of IoT Engagement.
[98] Please, note that in the context of this chapter the terms "regulation" and "legislation" are used interchangeably.
[99] See, for instance, Stanford Encyclopaedia of Philosophy, available at: https://plato.stanford.edu/search/search?page=1&query=Ethics&prepend=None

value of human dignity and prevent individuals being reduced to mere data subjects."[100] In this respect, IoT is considered to be one of the main technological trends, triggering concerns of ethical nature as, for instance, the likelihood of discrimination and the use of IoT devices in the health insurance sector.[101]

Standardization and Guidelines constitute forms of soft regulation that are quite commonly attempting to provide for technical matters and, more broadly, for the behaviour for organizations active in the domain of technologies, such as Cloud Computing. Soft law instruments such as the ones mentioned above do emerge from the original engagement of stakeholders, which –in most case- fades away later on, leading later on basically to them not being adopted in practice by the relevant stakeholders. Moreover, the effectiveness of soft law measures - as mentioned above - may vary due to a number of reasons. In any event, the common denominator of all these soft law instruments of is the potential lack of "real effectiveness" due to their voluntary nature and the related absence of redress mechanisms.

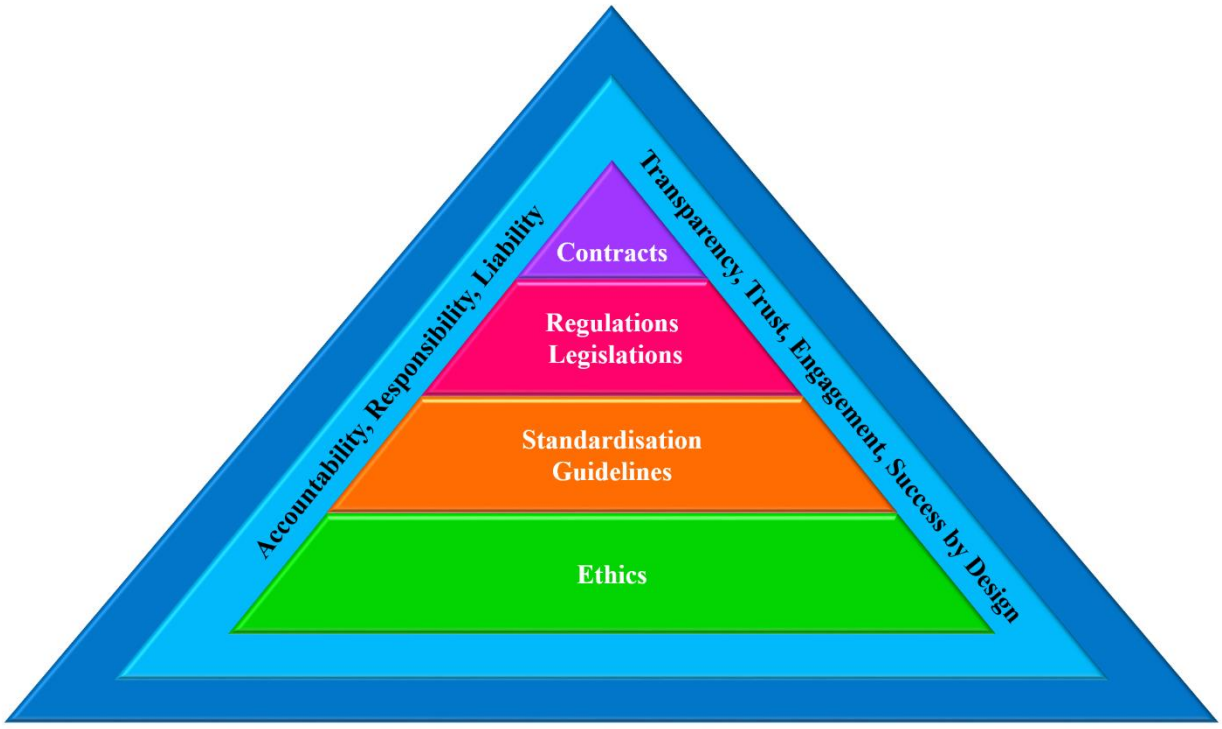


Figure 16: The hierarchy of engagement mechanisms

As opposed to Ethics and Soft Law instruments, Regulation and Legislation in essence impose stakeholders' engagement due to their mandatory nature. Interestingly, though, engagement in this case should not be mistaken as an equivalent to compliance, but rather as a safeguard for effective protection of all interests involved. Engagement in this case calls the entities assigned with the relevant responsibilities to go beyond the "mere box ticking" exercise of compliance and take all necessary action required in the context of responsible governance.

"Contracts can be defined as any legally binding agreement. The agreement gives rise to obligations to perform the promises made to the other party or parties to the contract, which are enforced and/or recognized by the law. The agreement is formed through an offer and acceptance between two or more consenting parties. If those agreements meet the requirements set in the context of each jurisdiction, which make them legally binding, they are contracts. Contracts

[100] See, also, https://edps.europa.eu/data-protection/our-work/ethics_en

[101] European Data Protection Supervisor, "Opinion 4/2015 Towards a new digital ethics Data, dignity and technology", available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf

specify what it is provided by national laws and/or provide, of course, for aspects not covered by the regulator. In any event, contracts cannot provide against what it stipulated by law (e.g. European Directives, national implementing laws)."[102] Note that there are differences between common law (e.g. UK, USA) and civil law jurisdictions (e.g. France, Germany) as to what it is precisely required in order for a contract to be valid.

The aforementioned engagement mechanisms form the implementing system of engagement within the IoT environment aiming – ultimately – at ensuring – among other noble goals – transparency, trust and accountability within the community of the IoT stakeholders. Nevertheless, it should be noted that first two engagement mechanisms identified, namely, one the one hand Ethics and, on the other hand, Standardization and Guidelines form an initial "testbed" of engagement, in the sense, that they cannot be enforced by authorities, thus, surfacing in a clear manner IoT stakeholders' "real" engagement to implement them.

A.3.2 The Regulatory and Contractual Relationships within LSPs

Both state-imposed law and contracts govern relationships between entities that can either be natural persons (e.g. acting in their capacity as consumers) or legal entities (e.g. companies or public-sector organizations). State imposed law, naturally, leaves no room for negotiation to the entities falling within its scope, while – as opposed to state-imposed regulation – contracts emerge from a negotiation process between the parties willing themselves to enter into a legal relationship. State imposed regulation and contracts form law assigning rights and responsibilities to the regulated entities and can be, therefore, enforced by courts.

As further explained below, the aforementioned Code of IoT Engagement mirrors earlier discussion. In particular, the Code of IoT Engagement is applicable to each and every entity wishing to become part of the community active within the Large-Scale Pilots (LSPs) and Coordination and Support Activities (CSAs) of the European Large-Scale Pilots Programme. Note that it is of great significance for stakeholders not only to identify themselves within those domains, but also to recognise in timely manner who are the other stakeholders that they may engage with in the future.

In particular, the IoT stakeholders include without limitation the following "entities" listed in detail below in random order:

- Society and environment
- Users
- Customers
- Non-users
- Data brokers
- Data providers
- Service providers
- Software providers
- Hardware providers
- Application developers
- Infrastructure providers
- Machines, interfaces and user-interfaces
- Universities and other knowledge institutions
- Standardisation development organisations

[102] Cloud Accountability project, ""D-4.3, Guidelines and tools for cloud contracts, available at: http://www.a4cloud.eu/sites/default/files/D44.3%20Guidelines%20and%20tools%20for%20could%20contracts_0.pdf

- Policy makers: governments, municipalities and others
- Authorities, law enforcement and intelligence services

Note that for the sake of this discussion, the notion of entities is being used "lato sensu", thus, including references to environment and society at large. In order to better depict the emerging relationships, the figure below groups the aforementioned entities into wider groups as follows:

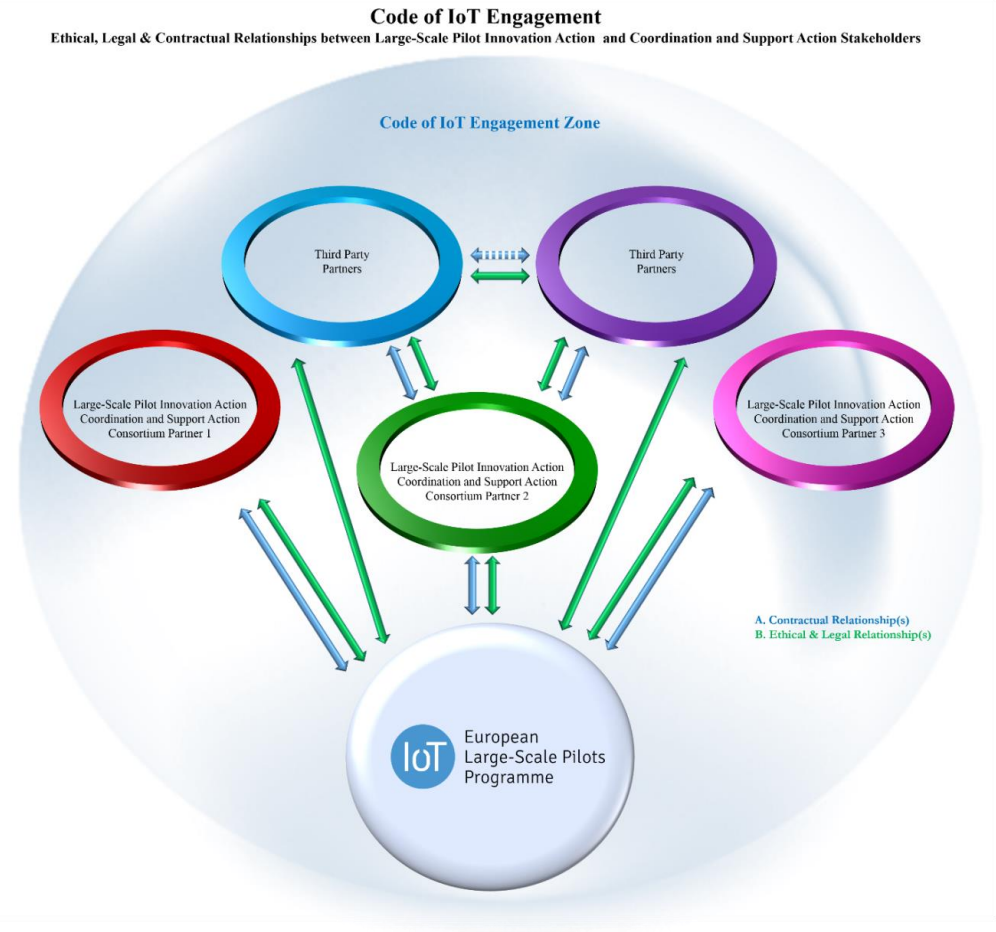


Figure 17: Code of IoT Engagement

In particular, the figure above captures how various stakeholders within the IoT Engagement Zone relate to each other. The figure illustrates the nature of relationships between the LSPs/CSAs and individual Consortium Partners. At the same time, it also visualises the nature of relationships between the LSPs/CSAs and parties that are no part of an LSP or CSA consortium (i.e. Third-Party Partners). To complete the picture, relationships between the Consortium Partners and Third-Party Partners, as well as between various Third-Party Partners are also accounted for.

As mentioned above, the Code of IoT Engagement is applicable to each and every entity wishing to become part of the community active within the LSPs and/or CSAs. Hence, it applies naturally to all relationships between the LSPs/CSAs and Consortium Partners, on top of other contractual and statutory obligations. In a similar way, the Code of IoT engagement supplements the contractual and statutory regime established between the LSPs/CSAs and the Third-Party Partners. However, while it is desired that Third Party Partners act and cooperate with LSPs/CSAs in accordance with the established ethical principles, often there is no direct contractual relationship between the individual LSP/CSA and the Third-Party Partner to ensure such compliance. Thus, the overarching and universally applicable Code of IoT Engagement serves to ensure compliance with ethical standards within the Zone, regardless or the relationship with the LSP or CSA.

A.3.3 The Challenges of Engagement

IoT stakeholders engagement constitutes quite a complex objective as it presumes organizational awareness, development of an organizational cultures that ensures the translation of norms and values into concrete practices, as well as, the investment of the necessary resources; the latter holds particularly true, as even mere compliance with strict rules can be costly, taking into account the expertise and the time required.

The section below touches upon the associated complexities for organizations by producing an overview of the difficulties relating to security that organizations will soon encounter in view of the upcoming legislation at EU level (e.g. ePrivacy Regulation) and the conflicts with the existing standards.

Setting the scene

Organizations in Europe will face regulatory complexity related to security in that they may be subject to the combined application of different legislative items regulating security obligations in the IoT domain.

The regulatory framework for security in the IoT domain consists of:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC GDPR)
b) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive")
c) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications" or "ePrivacy Directive")
d) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Here below the main provisions of each of the mentioned legislative act will be analysed in greater detail.

a) Key GDPR security provisions

- It applies to any organization, whether private or public, that processes personal data
- It imposes the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- It applies to data controllers and data processors alike
- It requires data controllers and data processors to enter into data processing agreements detailing the list of security requirements and obligations that the parties commit to respect;
- Data Controllers must notify supervisory authority of a security incident affecting personal data within 72 hours of becoming aware if feasible
- Individuals must be notified where an incident could cause serious harm
- Data Processors have the duty to notify data controllers "without undue delay"

b) Key NIS Directive security provisions

- It applies only to Operators of essential services and digital services providers

Operators of essential services are defined as private businesses or public entities with an important role for the society and economy.

Under the NIS Directive, identified operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

The **security measures** include:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services

Operators of essential services shall notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide, regardless of whether they affect personal data.

The Directives covers **digital service providers ("DSPs")** too. They are identified as:

- Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online)
- Cloud computing services
- Search engines

DSPs are under the obligation to implement security measures such as:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

The security measures taken by DSPs should also take into account some specific factors, to be further specified in a Commission implementing act due at the time that the current deliverable is being drafted. Note that all developments of significant importance will be discussed under the deliverables falling under the scope of "Task 05.03: Legal support, accountability and liability''.

- Security of systems and facilities
- Incident handling
- Business continuity management
- Monitoring, auditing and testing
- Compliance with international standards
- DSPs are also under obligation to notify security incidents the national supervisory authorities. Yet, differently from what is required to operators of essential services, they can take into account more criteria before performing the notification, such as:
  - Number of users affected (common with operators of essential services)
  - Duration of incident (common with operators of essential services)
  - Geographic spread (common with operators of essential services)
  - The extent of the disruption of the service
  - The impact on economic and societal activities
  - The rationale behind this difference in the provisions applicable to DSPs is that they shall be subject to a *light-touch set of rules.*

c) Key ePrivacy Directive provisions

- The security provisions of the ePrivacy Directive apply to providers of a publicly available electronic communications service and to provider of the public communications network.
- They must take appropriate technical and organisational measures to safeguard security of their services (…), having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

- In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.
- In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.
- When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

The ePrivacy Directive is currently under revision by the EU legislator; it will be replaced by a Regulation which will be aligned with the GDPR. A key aspect of the reform will likely be the extension of the ePrivacy norms from traditional voice, text and email services to: (i) "over the top" service providers; (ii) M2M communications (i.e. IoT technology); and (iii) probably all services with an electronic communications element. With this, players such as WhatsApp, Skype, Facebook or Messenger will also fall within the scope of the Regulation.

The definition of “electronic communication services” in the first version of the ePrivacy Regulation was rather broad as it could have been interpreted to include data transmission from one machine to another within its ambit. A later amendment modified this provision to distinguish between the application layer of M2M communications and the transmission layer which involves the conveyance of signals over via an electronic communications network. It was clarified that the latter would be considered as an electronic communication service and not M2M communications in general. Despite the amendment, there still seems to be some ambiguity about how these terms will be interpreted.

After the proposal was first published in January 2017, the draft went through numerous amendments. The most recent draft presented by the Finnish Presidency of the Council of the EU on 15 November 2019 was later rejected one week later by the Permanent Representatives Committee of the Council of the European Union (COREPER). It was stated that the inability to get the support of member states on crucial topics such as cookie walls, processing electronic communications data to combat child pornography and the like significantly contributed to the rejection. However, European Commission announced on 3 December 2019 that it will be presenting a revised draft as part of the upcoming Croatian presidency.

d) Cybersecurity Act

The EU Cybersecurity Act which came into force on 27th June 2019 strives to create a cybersecurity framework within the European Union in order to strengthen cybersecurity with respect to ICT products, services and processes. Recital 2 of the Act states that with the introduction of IoT, more and more devices are expected to be connected during the next decade. Moreover, it states that such connected systems have the capability of supporting all the aspects of our lives and boosting economic growth. Besides giving more teeth to the ENISA, the cybersecurity Act makes provisions for the following:

- Creation of European cybersecurity schemes based on European and international standards
- Voluntary self-assessment by manufacturers or providers of ICT products or services;
- Issuance of statement of conformity by manufacturer or provider of ICT products;
- Voluntary provision of EU statement of conformity, technical documentation and other related information pertaining to the conformity of the ICT service or product with the certification scheme to the designated national cybersecurity certification authority.

Consequences on the IoT operators

For the obliquity and wide potential of IoT deployments, IoT service providers may be subject to concurring security obligations under different sources of legislation. In their capacity as data controllers or data processors, they may be subject to the GPDR and, once the reform of the ePrivacy Directive is passed into EU law, to the new ePrivacy regime too. Given that IoT services may be part either of services provided by operators of essential services or by DSPs, IoT may be also caught by the rules of the NIS Directive. A case by case analysis is therefore needed to appraise to which legal regime they shall abide under the NIS Directive.

When this is the case, for example, IoT services providers will be subject to two concurring regimes as for what regards the notification of security breaches. They will have to be certainly notified to the relevant national authorities under the NIS Directive, and also the Data Protection Authorities if the breaches affect personal data.

The level of security to be provided will also vary depending on the qualification of the IoT service providers. Under both the GDPR and the NIS Directive, the concerned operators have to adopt security measures which are "*appropriate and proportionate to the risk*". Even so, risks will have to appraised and mapped differently, and therefore security measures applied under the GDPR and the NIS Directive may overlap to some extent, but not entirely.

A.4 The IoT Security and Privacy Framework[103]

This section produces an overview of the IoT security and privacy engineering framework, being a constitutive component of the broader IoT Policy framework.

A.4.1 Privacy

Taking into account the nature of privacy as a fundamental human right[104] and in view of best surfacing the human centred nature of the privacy framework per se –being part of the overarching human centred IoT Policy Framework proposed, the analysis below starts by using as a benchmark point of reference the user centred concerns associated with privacy. It further touches upon the basic requirements of European Data Protection Law (e.g. principle of data minimization, privacy by design etc.). Note that for the sake of the present discussion, the concepts of privacy and data protection are being used interchangeably.

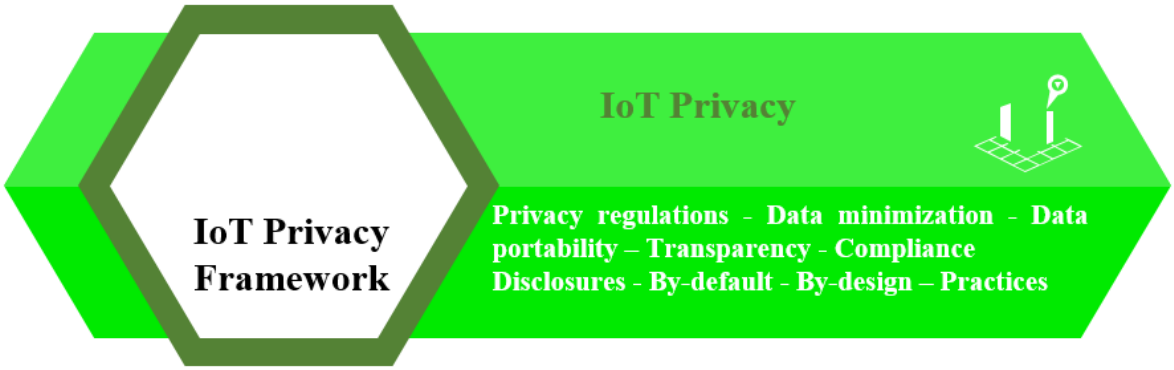


Figure 18: IoT Privacy framework[105]

[103] This section was separated into two parts in deliverable D05.01

[104] Articles 7 and 8 of the Charter of Fundamental Rights of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[105] The concepts mentioned in the figure relate to the GDPR, discussed –to an extent- under the present chapter, though, they are not all of them addressed separately.

The panorama of user centred concerns

Sensors, mobile phones, wearable objects, RFID tags, cameras, middleware components, have a common feature: they are all points of entrance of data, often personal data. As the players of the IoT landscape heavily leverage on personal data to deliver services and increase consumers' welfare, personal data protection and security are key elements in the "value creation chain" of IoT.

In this regard, IoT does not necessarily pose new challenges; it – however – makes traditional challenges escalate and multiply. For example, data subject's control on personal data becomes more difficult due to the dispersed number of data sources and entities processing personal data; as the chain of providers of IoT services stretches, allocation of responsibilities and enforcement of data protection law become more complex than before; and the same can be said with regards to compliance to the principles of purpose limitation and data minimisation. Plus, it is not easy to identify in each case what the viable legal ground for personal data processing is. The data subject's consent is not always a reliable one; in some cases – especially in the Smart Cities domain – Union or Member State law may constitute the legal basis for personal data processing through IoT deployments.

There is therefore an underlying relation between the need of privacy and the consequential need of trust in the IoT architectures handling our personal data, which renders necessary to make the IoT trustworthy and the data processing operations taking place therein transparent.

The need for privacy can thus be categorized around the following subcategories:

- **Identity Privacy**: The need of privacy for information that can identify a person.
- **Location Privacy**: The need of privacy for information that can identify a person's location, since the location is in itself personal data which can reveal further personal data, e.g. points of interest
- **Footprint Privacy**: The need of privacy for all personal data leaked unintentionally, e.g. preferred language[106]. To these subcategories a further one should be added:
- **Dynamic Privacy**: The need to keep control on the processes of profiling, inferencing and automated decision making started from the collected personal data, which can be further categorized in:
  - **Device Trust**: Need to interact with reliable devices.
  - **Processing Trust**: Need to interact with correct and meaningful data.
  - **Connection Trust**: Requirement to exchange the right data with the right service providers and nobody else
  - **System Trust**: Desire to leverage a dependable overall system. This can be achieved by providing as much transparency of the system as possible[107].

According to an elaboration made by IoT-EPI, the relation between privacy and trust in IoT can be defined with Figure 19 below:

This graph represents the required trust levels given a certain need for privacy. There we see that even when the need for privacy is at a maximum, at 1, the required trust level towards a service / architecture is below 0.75.

Such a mismatch is due to the fact that for users it is impossible to trust a service / architecture 100% since there are too many unknown factors in the current state of things. An individual

[106] Daubert, Jorg, Alexander Wiesmaier, and Panayotis Kikiras. A View on Privacy & Trust in IoT. Tech. AGT International, Germany, Telecooperation Group, Technical University of Darmstadt, Web. <https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/joerg15privacytrust.pdf>

[107] Ibid.

sharing personal data usually does not have a complete understanding of how the architecture is built up, about how security measures are realised or how trustworthy potentially involved third parties are. The graph also implies that that the user is not able to trust the service at the expected level in relation to his privacy needs – leaving room for improvement on the side of IoT device and software vendors. IoT-EPI researchers have therefore included an "Ideal Trust" line in Figure 19 to indicate the user trust levels that vendors should be striving towards.[108]

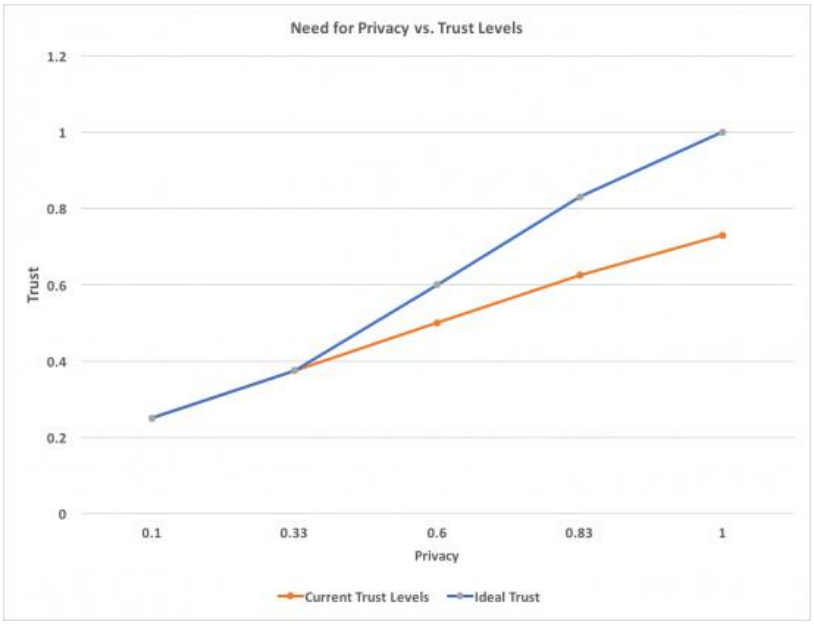


Figure 19: Relation between privacy and trust

The biggest challenge for IoT is therefore to fill this information asymmetry with users by means of technical and organisational user-friendly solutions.

One idea could be to deploy a **solution which measures the level of trustworthiness of a service using the traffic light metaphor**. Alternatively, a more elaborate dashboard could be used to give the user an overview of trust values and make adequate suggestions about which services to use[109].

Yet in some different contexts, like in the smart cities domain, users should be involved when carrying out **Privacy Impact Assessments** on the envisaged smart city initiative.

In fact, According to Article 35 (9) of Regulation 679/2016 on the processing of personal data (GDPR) "*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*".

This can be done through:

- Open Consultation of users (citizens/data subjects)
- Meetings or workshops with the data subjects' representatives
- Other measures aimed at tackling trust and privacy issues of users could be:
  - Anonymizing as much as possible; alternatively, personal data should at least be pseudonymized;

[108] "The need for Privacy and its relation to Trust in the Internet of Things", http://iot-epi.eu/2017/08/10/privacy-and-trust-in-iot/.

[109] Leister, Wolfgang, and Trenton Schulz. Ideas for a Trust Indicator in the Internet of Things. Tech. IARIA, 27 May 2012. Web. <https://www.thinkmind.org/index.php?view=article&articleid=smart_2012_2_10_40043>

- Setting a clear retention and portability policy for personal data processed by IoT services;
- Informing users on the envisaged data processing operations, as well as on the stakeholders involved, by means of dashboards.

Furthermore, CREATE-IoT has leveraged on several data protection related resources and tools that are developed by European research projects to strengthen user's acceptance, including:

1) Serious game on data protection for IoT

U4IoT has developed a serious game on IoT and data protection. The game will be used to raise awareness and educate the various stakeholders on the risks and obligations related to data protection when deploying IoT.

2) Privacy by Design Crowdsourcing Application

The IoT Lab European research project (www.iotlab.eu) developed a privacy-by-design smartphone application to perform crowdsourcing and collect end-user feedbacks in IoT testbeds, while ensuring a complete respect and protection of their personal data. The IoT Lab application is being redesigned by the U4IoT European research project in order to more specifically address the needs of the various IoT Large-Scale Pilots (LSPs). This new app is likely to be used and tested for collecting anonymized end-user feedbacks on Synchronicity IoT deployments.

3) EuroPrivacy Certification

The Privacy Flag European research project has contributed to the development of a European Certification Scheme on personal data protection named EuroPrivacy (www.europrivacy.org). EuroPrivacy has been used in the context of the City of Carouge (one of the Synchronicity reference zones).

4) European Privacy Portal

One of the partners of the Privacy Flag European research project has developed a European Privacy Portal (www.privacyportal.eu) that has been used to promote the Synchronicity privacy enablers.

Data Protection by Design: the overarching privacy principle

The Directive 95/46 – widely known as the Data Protection Directive – and the GDPR introduce a set of principles that should underlie the processing of personal information under EU Law. Those include principles such as the principle of data minimization[110] and the principle of purpose specification.[111] This section, though, puts emphasis on the principle of "Privacy by Design" that constitutes a newly introduced principle under Article 25 of the GDPR.

In particular, it has been argued that in order to implement a sound data protection approach within IoT, the key is to adhere to privacy-by-design in advance[112]. Taking into account the aforementioned regulatory instruments and the associated challenges identified within the IoT environment, the basic set of principles for privacy-by design- are captured in the figure below:

[110] The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it. See, also, https://edps.europa.eu/node/3099#data_minimization

[111] See also Article 5 (1) (b) of the Data Protection Directive and the General Data Protection Regulation (GDPR).

[112] O. Vermesan and J. Bacquet (Eds.). Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.

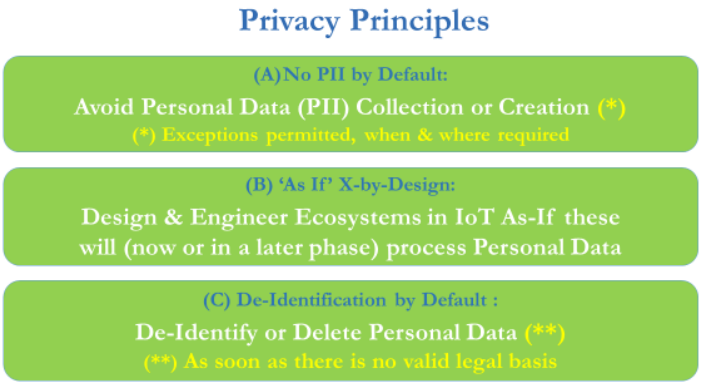


Figure 20: Privacy Principles

In particular:

- *No personal data by default* implies refraining from any collection or creation of personal data by default, except for cases where such collection or creation is legally required and to the exact extent required.
- *'As-If' X-by-Design* refers to the requirement that ecosystems are designed and engineered as-if these will process personal data at an immediate and/or later stage.
- *De-Identification by Default* refers to the de-identification, sanitization or deletion of personal data as soon as the legal basis for keeping such data ceases.
- *Data Minimization by Default* stipulates that personal data shall only be processed where, when and to the extent required; otherwise this data shall be deleted or de-identified.
- *Encryption by Default* refers to the requirement to encrypt personal data by default, while capturing both digital rights and digital rights management.

The close interconnection between privacy and security

The concepts of security and privacy, while exhibiting a complex and nuanced mesh of interrelationships, which includes touch points and areas of overlap, are different. A common misconception consists in the identification of confidentiality (one of the key constitutive concepts or goals of the information security triad, see definition given in ISO/IEC 27000:2009[113] with privacy.

Several classical security techniques can be instrumental in enhancing privacy and personal data protection[114]. For example, data encryption cryptographic algorithms, hashing functions/digital signatures, and server mirroring (combined with effective identity and access management solutions that protect from unauthorized access and use) can help to ensure confidentiality, integrity and availability of personally identifying information. Proxy re-encryption, malleable signatures or homomorphic encryption are examples of newer security approaches to secure sharing or processing in untrusted environments of such data.

While security techniques are indeed relevant to support data protection and privacy, they do not guarantee per se the principles of privacy[115]. For instance, an e-Commerce transaction may be secured with https protocol but fail to apply the principle of data minimisation or, in the context

[113] ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC

[114] The General Data Protection Regulation establishes the obligation for data controllers and processors to provide a description of the technical and organisational measures needs in the record of processing activities (Art. 30), and this is also a key element of Data Protection Impact Assessments (Art. 35, paragraph 6 (d)), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[115] See https://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html

of IoT, a device may be collecting and/or storing more data than is needed to provide a service e.g. relying on raw data rather than aggregated data[116]. Furthermore, some approaches to security which could be justified in some contexts as necessary, can nonetheless be detrimental to privacy goals and principles, for instance security checks (in particular body scanners) or boarding checks in airports (no anonymity allowed), or design choices e.g. use of stable identifiers in wearable things, may limit data subjects' possibilities to remain anonymous[117]. Thus, depending on a number of complex socio-ethical and even political factors in the specific contexts of application, security and privacy goals may be aligned or at different degrees of conflict. This relates to the notion of privacy being a fundamental right protected in Articles 7 and 8 of the Charter of Fundamental Rights of the EU[118], but not an absolute value inasmuch as context determines if and how it should be applied[119]. In fact, restrictions are contemplated as well to the application of data protection principles and data subjects rights in the General Data Protection Regulation[120] e.g. "when necessary and proportionate in a democratic society to safeguard: national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties […]".

In order to classify the possible relations between security and privacy we can consider the **four world views** proposed by Wolfgang Hofkirchner[121]: reductionism, projectionism, dualism and dialectic. A suitable representation of them, along orthogonal axes, is provided in the figure below, where horizontal axis reflects a zero-sum or mutually exclusive trading-off of security vs privacy while the vertical axis considers alternative possibilities in the security-privacy relation:

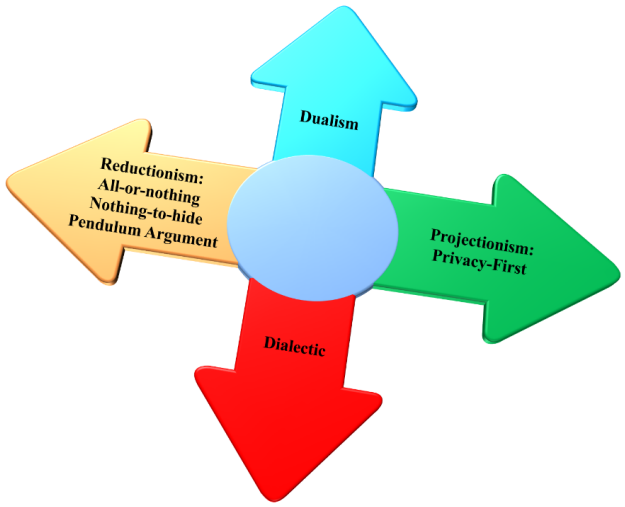


Figure 21: Relationship Privacy-Security

In the **reductionist** approach, security dominates privacy, that is, deprivation of rights to personal data protection i.e. indiscriminate surveillance, is justified on the grounds that well-behaving individuals should have "nothing to hide", that security is mutually exclusive of privacy in a zero-sum trade-off ("all or nothing") or that in times of crisis it is necessary to sacrifice or restrict human rights ("pendulum" argument). At the opposite end, the **projectionist**

[116] See pp, 19, 23 of Article 29 Data Protection Working Party, WP223, Opinion 8/2014 on the on Recent Developments on the Internet of Things, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[117] Ibid., p.8.

[118] Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[119] Nissenbaum, Helen. 2010. Privacy in context. Stanford, CA: Stanford University Press

[120] See Art. 23, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[121] Hofkirchner, Wolfgang, 2010. Twenty questions about a unified theory of information. Litchfield Park, AZ: Emergent Publications

approach values privacy as an absolute good which must be preserved at the expense of security and even the common good of society. In the **dualistic** approach, security and privacy are seen as completely autonomous variables and is often related to the views on privacy by design advocated by former Ontario's Information and Privacy Commissioner Ann Cavoukian where privacy enhancing technologies can maximize both privacy and security. Finally, the **dialectical** approach tries to address, from human security concept that takes into account a broader view of the elements that cause instability and conflict in our global world, trying to address root causes of problems affecting common people and moving away from simplistic solutions based on technologies and law & order policies[122].

As an integrally constitutive part of the IoT Security Framework we propose, there is clear need to consider a **principle-based approach to security and privacy**. In this respect, in addition to data protection principles and security principles and measures explicitly mentioned in the GDPR (Arts. 5-11 and 32)[123], we consider standard ISO 29100[124], which defines a privacy framework provides a set of concepts (actors and roles, interactions, recognizing Personally Identifiable Information, privacy safeguarding requirements, privacy policies; and privacy controls) and a set of privacy principles: 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. As proposed in paper "A Privacy Engineering Framework for the Internet of Things"[125], additional principles should be added from an engineering viewpoint to this framework towards transforming it into a **privacy engineering framework** suitable to address the lifecycle of privacy controls and policies, with due consideration of privacy engineering principles and safeguards, actors' roles in the engineering process, use of common privacy engineering terms, among others[126]. The additional engineering principles described in this paper include the integration of risk management, compliance, goal-orientation (in requirements phase), data and process oriented design strategies, comprehensive lifecycle support as well as privacy-related objectives (unlink ability, transparency and intervenability)[127].

Further to this, a **privacy and security by design engineering methodology** is needed in order to make the above-mentioned principles from the privacy engineering framework operational in IoT systems and subsystems. For instance, the FP7 PRIPARE project[128] proposed a methodology[129] combining privacy risk analysis with a goal-oriented elicitation of operational requirements, integrates architecture-related decisions with PETs and privacy controls as a result of the design process and can be applied to cover entire IoT systems and subsystems (in the latter case focused on enabling features for building privacy control at integration time) engineering lifecycle, integrating with different mainstream development technologies.

[122] Please see a more complete discussion of the four views in pp.4-8 of Research Paper #6, Privacy and Security in Europe, Fuchs C., The Privacy & Security Research Paper Series, PACT Project, May 2013

[123] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[124] International Organization for Standardization (ISO), Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition, Geneva, 15 Dec 2011.

[125] See pp. 24-25, Kung A. et al. (2017) A Privacy Engineering Framework for the Internet of Things. In: Leenes R., van Brakel R., Gutwirth S., De Hert P. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, vol 36. Springer, Cham, https://link.springer.com/chapter/10.1007/978-3-319-50796-5_7/fulltext.html

[126] Ibid, p. 6

[127] Ibid. p. 24

[128] http://cordis.europa.eu/project/rcn/110590_en.html

[129] See http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

The relationship between security and privacy (see Figure 4) is the following[130]:

- Security risks arise from unauthorized system and user behaviour. Many security risks are not privacy risks, for instance the protection of an organisation confidential data;
- Privacy risks arise from unauthorized personal data processing (e.g., lack of proper consent management mechanisms, lack of security of collected personal data such as health data);
- Privacy risks arise as a by-product of unauthorized personal data processing (e.g., re-identifying a data set to an individual).

A.4.2 Security

This section expands on the creation of an appropriate security framework for a human centred IoT. To this end, the analysis focuses on "secure systems", which –in the context- of the discussion below refer to the systems that are currently found in the "*state of being free from danger or threat*[131], or systems which are *not likely to fail or be lost*.[132]"

Taking into account that human centred computing is often defined as the study of systems mixing human and computing systems involving human interactions, human centred design, and human empowerment, the analysis to follow focuses on human centred IoT systems.[133]

Note that the term security is used as an overarching term that subsumes other terms, including ICT security. Instead of the term security framework, we have also considered using the term dependability framework.

Due to the strong domain connotation of the term "dependability[134]", though, referring to fault tolerant systems or safety critical systems, the term "security" was considered most appropriate.

The construction of the framework is based on the following approach: security, dependability and privacy properties must be applied throughout the lifecycle processes of IoT systems. This includes impact assessment (when risks are assessed) and design of controls (when risks are mitigated).

The obtained security framework also includes the necessary assurance of the processes to allow for trust.

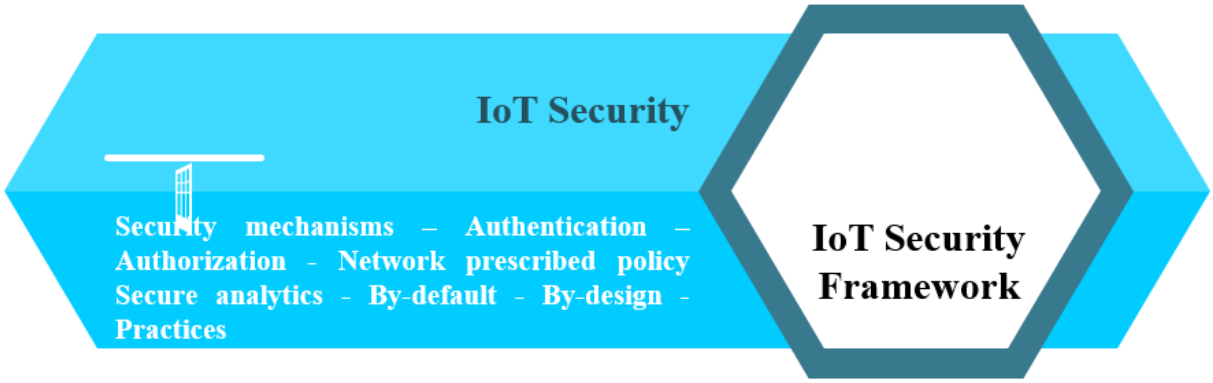


Figure 22: IoT Security Framework

[130] From ISO/IEC 27550 Privacy engineering for system lifecycle processes.
[131] https://en.oxforddictionaries.com/definition/security
[132] http://dictionary.cambridge.org/dictionary/english/security
[133] The Cambridge dictionary states that *human centred* is an adjective used to describe systems that are *designed to work in ways that people can easily understand and learn. See, also,* http://dictionary.cambridge.org/dictionary/english/human-centered
[134] Dependability is the *ability to deliver a service that can justifiably be trusted*. Another definition of dependability is the *ability to avoid service failures that are more frequent and more severe than is acceptable.*

Objectives of framework

As showed in Figure 23, the IoT security framework has to take into account the following elements:

- Ensuring IoT security mechanisms
- Ensuring IoT data protection
- Ensuring IoT system resilience
- Providing IoT system/application trust

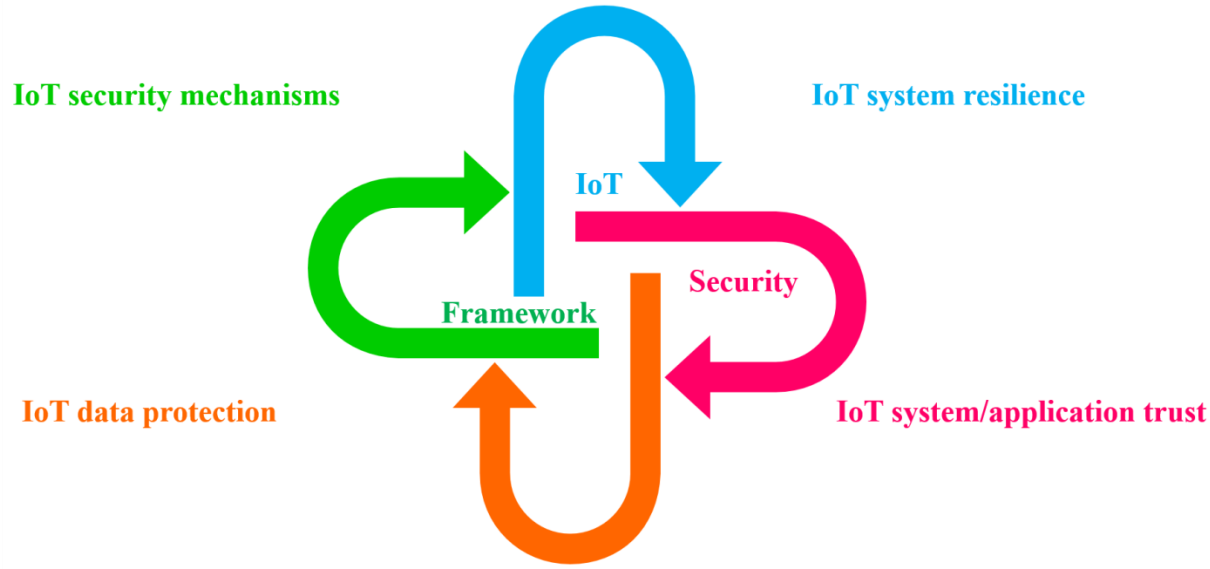


Figure 23: Key Objectives of a Security Framework for a human Centred IoT

Figure 24 shows the relationship between the key objectives: data protection and resilience are the two pillar objectives concerning dependability in IoT systems, while trust is associated with the accepted level of dependence.

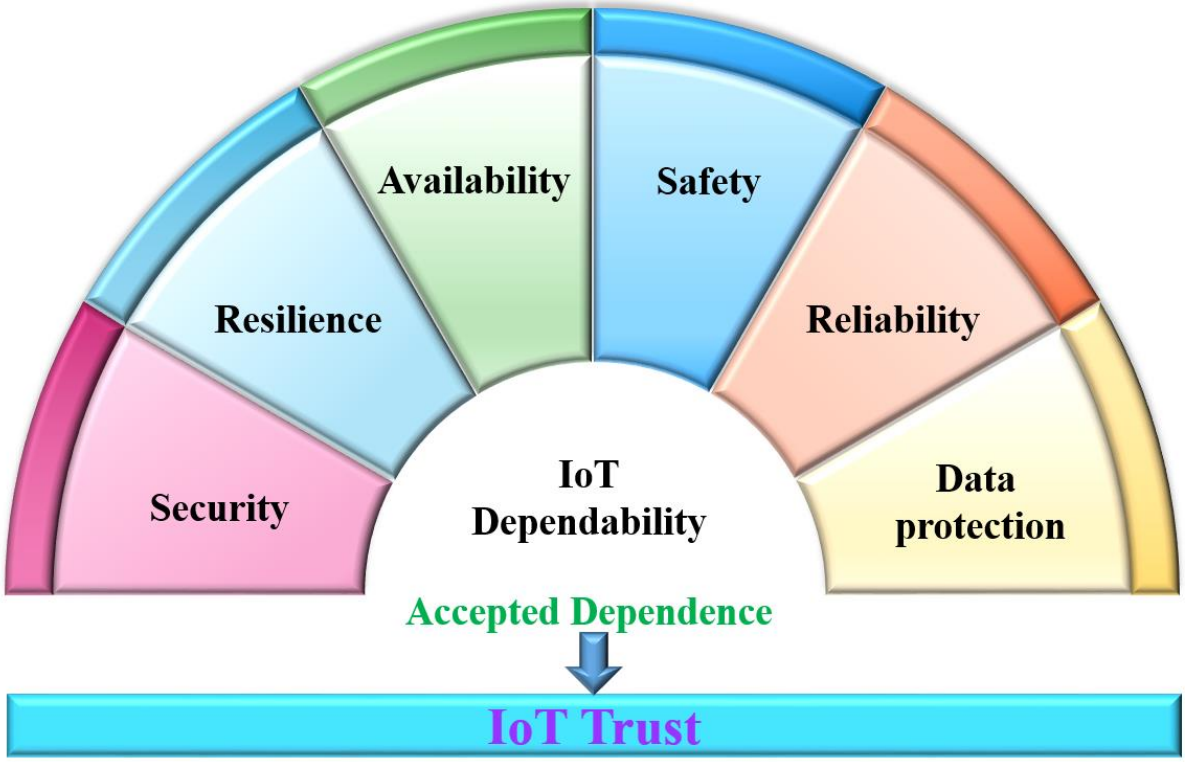


Figure 24: Trust - Accepted dependence

Security, Dependability and Privacy Properties

The following properties have been proposed for security, privacy and dependability.

- Properties for security are often based on the established CIA triad of confidentiality, integrity, and availability:
  - Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Examples of measures for achieving or enhancing confidentiality include protected transmission of collected data, protected access with suitable authentication schemes, protected processing of data, and protected storage.
  - Integrity ensures the accuracy and completeness of data over its entire life cycle. Examples of measures for achieving or enhancing integrity include schemes such as digital signatures.
  - Availability ensures accessibility and usability upon demand by an authorized entity. Examples of measures for achieving or enhancing availability include preventing service disruptions due to power outages, hardware failures, or security denial of service attacks using schemes such as redundant systems.
- Properties for dependability are often based on the landmark paper published in 2004 combining security and dependability[135]:
  - The CIA triad (Confidentiality, Integrity, Availability)
  - Reliability, defined as continuity of correct service
  - Safety defined as the absence of catastrophic consequences on the user(s) and the environment
  - Maintainability defined as the ability to undergo modifications and repairs
- Three properties have been defined for privacy[136], unlinkability, transparency, intervenability. They are presented as the extension of the security triad:
  - Unlink ability ensures that a use may make multiple uses of resources or services without others being able to link these uses together. The objective of unlink ability is to minimize the risk to privacy created by the potential linking of separate sets of personal data, for instance a customer uses two different accounts for navigation and for telephone calls.
  - Transparency ensures that an adequate level of clarity of the processes is reached so that the measures taken during the lifecycle for security and privacy can be understood and reconstructed at any time. Transparency covers the entire system life cycle. Transparency allows stakeholder to reconstruct and improve the legal, technical and organisational setting in case it is needed, for instance when there is a security or privacy breach.
  - Intervenability ensures that relevant partners can intervene in security and privacy operations. The objective of intervenability is to provide the possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing. This can possibly involve the application of corrective measures and counterbalances where necessary, for instance requesting for data erasure, withdraw consent.

Life Cycle Processes for Security, Dependability, Privacy

In order to meet the objectives of the security framework, a number of processes must be integrated as showed in Figure 25 must:

- Impact assessment (focus is on risk analysis activities)
- Controls (focus is on the measures)

[135] . Avizienis, J.C. Laprie, B. Randell, and C. Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on dependable and secure computing, vol.1, n°1, Jan-March 2004.

[136] Marit Hansen, Meiko Jensen, Martin Rost: "Protection Goals for Engineering Privacy"; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf.

- Assurance (focus is on activities that are aimed in raising confidence).

We have singled out these processes, because:

- They are the pillar processes to achieve data protection, resilience, trust,
- They will involve substantial development and organisation resources,
- They will affect profoundly the design, deployment and operation of IoT systems.

In particular**, Security, dependability and privacy impact assessment in life cycle** analyses the effect of vulnerabilities concerning data protection, resilience and trust in IoT systems:

A data protection impact assessment corresponds to the analysis of risks concerning data protection (e.g. unauthorised personal data processing), their consequences (e.g. privacy breach) and their mitigations (e.g. minimizing data collection),

A resilience impact assessment corresponds to the analysis of risks concerning ICT security (e.g. denial of service of the electricity grid), their consequences (e.g. essential services not available) and their mitigations (e.g. incident response measures),

A trust impact assessment corresponds to the analysis of risks concerning trust vulnerabilities (e.g. lack of transparency at the governance level), their consequences (e.g. lack of trust on some applications/solutions/stakeholders) and their mitigations (e.g. providing an information desk for citizens, setting up a citizen engagement process). This is a higher-level assessment that is not widely promoted, nor defined.

Security, dependability and privacy controls in life cycle correspond to a focus on organisational and technical measures for security, dependability and privacy in the life cycle of IoT systems:

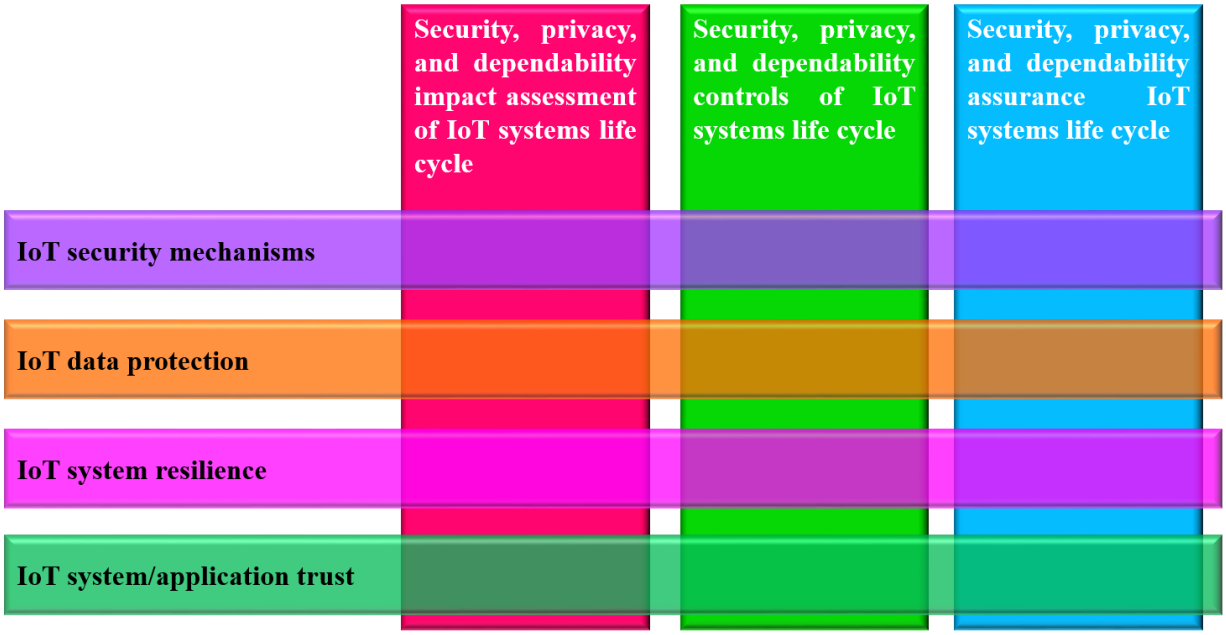


Figure 25: Lifecycle processes for security, dependability and privacy

The integration of data protection corresponds to privacy-by-design (e.g. the definition of ISO/IEC 27550 privacy engineering) and to data protection by design and data protection by default as stated in the GDPR.

The integration of resilience corresponds to cybersecurity (e.g. the NIST cybersecurity framework[137], or the NIST publication on systems security engineering[138]), with definition of phases such as Identify, Protect, Detect, Respond, Recover.

The integration of trust corresponds to trust-by-design (e.g. transparency capabilities, empowerment capabilities, accountability practice). It can be argued that trust-by-design integrates data protection and resilience. For instance, data protection compliance could require data controllers to keep a registry of all personal data processing activities.

Security, dependability and privacy assurance in life cycle corresponds to processes to ensure that IoT systems meet a defined level of data protection, resilience and trust:

Data protection assurance corresponds to the activities that will help demonstrate that a given level of data protection is reached. This can involve privacy impact assessment audits, privacy engineering audits, interoperability verification activities (e.g. user expresses privacy preferences, which must be shared by multiple application providers), or certification activities[139].

Resilience assurance corresponds to the activities that will help demonstrate that a given level of resilience is reached. This can involve security assurance and audits and certification (e.g. common criteria evaluation). Resilience depends on the services. For instance, resilience of essential services (e.g. finance, electricity) will necessitate more stringent levels.

Trust assurance corresponds to the activities that will help demonstrate that a given level of trust is reached. This can involve transparency assurance activities (e.g. verifying that a citizen privacy breaches complain is properly handled or verifying that a registry of personal data processing activities is compliant with GDPR).

Assurance refers to processes that are largely influenced by policies from data protection authorities (for data protection and GDPR compliance) and national security centres (for resilience and the NIS directive).

Organisations and roles in the processes

IoT systems involve a complex ecosystem of stakeholders. This is because many such systems are systems of systems. For instance, autonomous vehicles are systems that are integrated in a higher transport system infrastructure.

It is therefore important to provide a categorisation of the main roles in the ecosystems, as individual organisations specialised in a given role will use the security framework in IoT from different viewpoints.

Figure 26 shows an example of categorisation:

- Suppliers provide the technologies and components that will be integrated in an IoT system. Such suppliers have one main objective: meeting the needs of a market. When it comes to the security framework in IoT, these suppliers are expected to provide capabilities that will be useful to meet the requirements associated with trust, data protection and resilience, for instance a storage system could include access right management capabilities.
- Integrators select suppliers' products and integrate them in order to deliver an IoT application. The integrators play a key role in selecting and developing properly the capabilities underlying the security framework in IoT

[137] https://www.nist.gov/cyberframework

[138] http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

[139] This will be depending on policies. For instance, it is a general practice that safety oriented application are subject to certification schemes.

- Operators are responsible for the deployment, maintenance or removal of IoT applications. Hence, they are responsible for the provision of the right level of trust, data protection and resilience.
- Authorities provide overall governance. This governance can be limited to regulation supervision (e.g. consumer market applications), or it could involve significant responsibilities (e.g. smart city applications).

The observance of the security framework in IoT systems is made difficult by:

- Multiple levels of stakeholders (e.g. data controllers and data processors concerning data protection),
- Multiple supply chains (e.g. electric vehicles involve the smart grid supply chain, the automotive supply chain, and the ICT supply chain);
- Multiple interoperability requirements (e.g. an application can access similar devices)
- Multiple system lifecycles (e.g. integrating new systems with legacy systems).

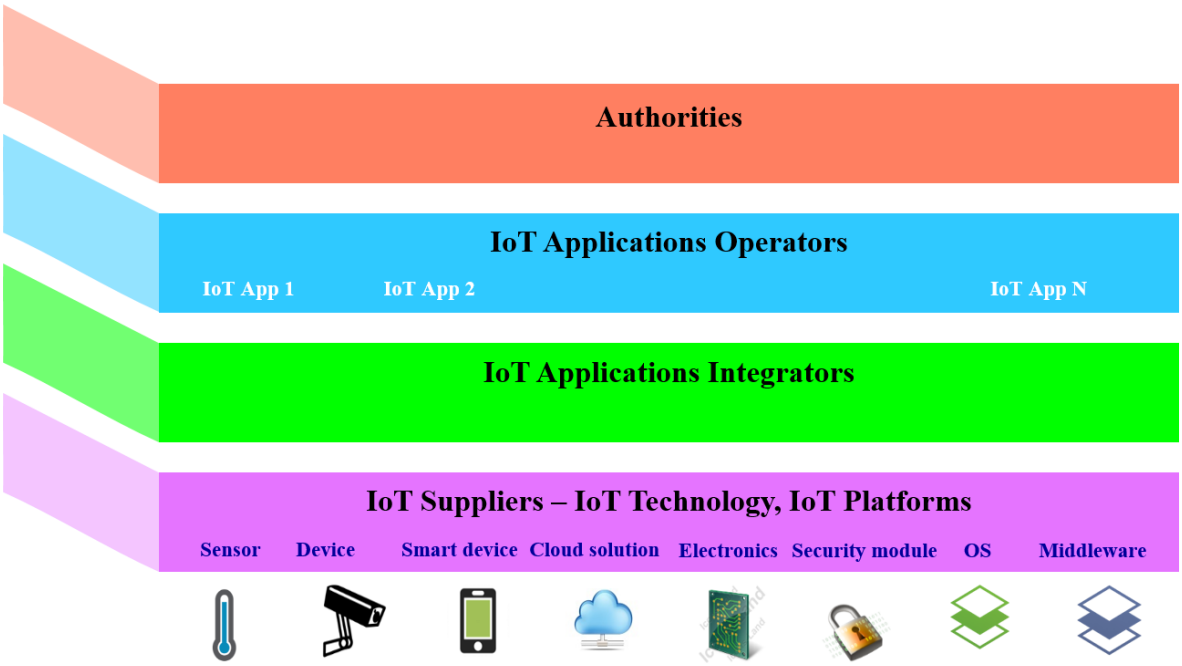


Figure 26: Organisations and roles in the Secure Framework for IoT

Consequently, it is necessary to optimise the positioning of each individual stakeholders, suppliers, integrators, operators and authorities with respect to the security framework:

- Key components: trust, data protection, resilience
- Associated processes: impact assessment, control design and assurance

Integrating organisation and roles in IoT Architectures

The security framework points out the importance of organisations and roles in the security framework. This emphasis is also visible in current standardisation initiatives:

- On IoT standards

  - The current standard being developed on an IoT reference architecture (ISO/IEC 30141 integrates a so-called usage view. It defines the following roles: IoT service provider, IoT service developer and IoT-user.
  - Current discussions which will lead to the creation of a new standard on security and privacy guidelines for the IoT is likely to take a lifecycle viewpoint[140].

- On big data standards
  - The current standard being developed on a big data reference architecture (ISO/IEC 20547-part 3) defines the following roles: data provider, big data framework provider, big data service partner, big data application provider, big data consumer.
  - The current standard being developed on big data security and privacy (ISO/IEC 20547 part 4) defines the following roles: big data security and privacy planner, big data security and privacy manager, big data security and privacy implementer, big data security and privacy operator, big data security and privacy auditor[141].

- On smart city standards
  - The current standard being developed on smart city business process framework (ISO/IEC 30145-1) defines a specific process on safety, security and resilience which follows the following principles
    - Holistic approach
    - Aggregation data from multiple sources to manage safety, security and resilience
    - Elaboration of deployment of data privacy standards
    - Separation between critical and non-critical services of the city so that services can be engineered accordingly
    - disaster recovery plans that are regularly tested

This is also visible in current research initiatives. For instance, the CTI French SystemX project on cybersecurity for intelligent transport is currently investigating a common ITS architecture, identifying three types of isolation: certified/non- certified isolation, safety/non safety isolation, critical/noncritical isolation.

The main security domains of IoT

Figure 10 shows how IoT systems can be decomposed into different segments.

The segments address several areas as explained below:

- The vision is that there are IoT applications which take advantage of features provide by things.
- IoT applications consist of algorithms and data. Examples of algorithms are smart applications, analytics. Examples of data are personal data, business data and metadata.
- Things consist of computing facilities and machines. Examples of computing facilities are cloud computing, network devices, edge computing. Examples of machines are robots, vehicles, drones, wearables, sensors.

The rationale for defining security domains is to provide a taxonomy to allow for comprehensive risk analysis (for trust, data protection and resilience). Figure 27 provides another categorisation for complex systems such as vehicles, drones or rail systems: perception means, communication channels, embedded devices, on-board storage and shared services.

[140] The following phases are proposed by the Japanese contribution: establish policy, identify risks, apply secure design basics, apply network controls, maintain security.

[141] E.g. the manager typically focusses on impact assessment, and institutional and life cycle integration. The auditor focuses on assurance.

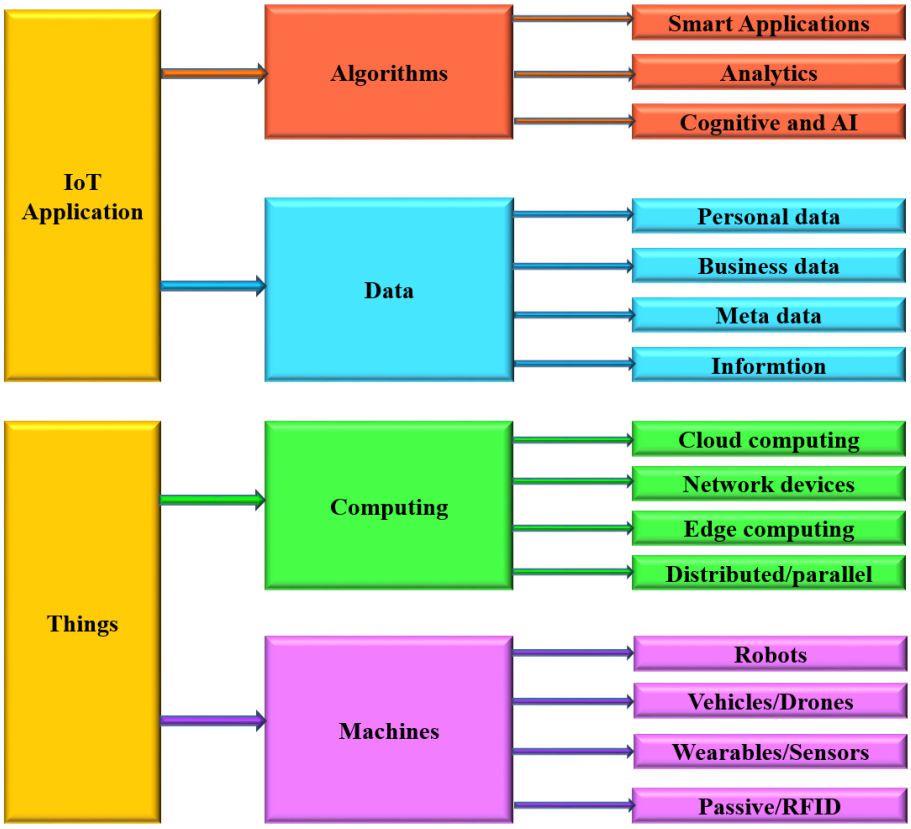


Figure 27: Security Domains of IoT

A.5 SOTA Methodology

Further information is described in related background documents.

Proposed SOTA methodology

This section describes an initial security methodology called SOTA (state of the art) that was presented to large scale pilots in a number of webinars. The methodology aims to facilitate organizations' compliance by design with these legal developments.

The methodology -relevant for both public and private organizations- recognizes that every IoT ecosystem consists of core a stack of layers and dimensions (including, among others, the user, data, application and infrastructure). It is created on the basis of thorough examination and reviewing of numerous relevant standards, guidelines, best practices, frameworks and other resources developed and made publicly available by various stakeholders, including the U.S. Department of Homeland Security, National Institute of Standards and Technology and other organizations.

The subsequent systemizing and segmenting have resulted in identification of almost 400 unique security principles which have been plotted against the appropriate layers and dimensions. The relevance of individual principles to stakeholders varies with respect to context, i.e. the stakeholder's role in the ecosystem and domain. Based on a couple of simple criteria, an individual stakeholder can utilize the methodology and use it as a tool to produce a set of relevant and applicable principles to ensure state-of-the-art cyber security.

In particular, State-of-the-Art security of IoT ecosystems is essential for achieving high-level security as well as sustainability and durability of these ecosystems.
It has been recognized that IoT ecosystems consist of the following layers (numbers 3, 4, 5 and 7 below) and dimensions (numbers 1, 2 and 6 below) where dimensions may be relevant in one, more or all layers:

1. User/Human factor
2. Data
3. Service
4. Software/Application
5. Hardware
6. Authentication
7. Architecture/Network

When determining and implementing applicable SOTA principles, an organisation should carefully assess these principles while taking account of every individual layer and dimension. Especially, organizations should approach both security and privacy from the "by design" perspective, requiring IoT devices to take security- and privacy-related requirements into consideration already at the stage of their early design.

On the one hand, by doing so, an organisation will be able to demonstrate that it is a mature, aware, accountable and relevant market player, and thus establish the desired level of trust with its partners and customers. On the other hand, many of the presented principles are reflected in mandatory legal requirements contained in new tech-related laws applicable as of 2018 (including the General Data Protection Regulation and the Directive on Security of Network and Information Systems).

The relevance of SOTA principles is based on the organisation's answers to the set of questions mentioned below. These have been found relevant and selected from a repository of almost 400 unique and individual principles identified in numerous sufficiently mature standards, guidelines, best practices, frameworks and other resources published by various governments, government agencies, state bodies, industry associations, international organizations and other relevant stakeholders.

The SOTA paradigm

The set of SOTA principles outlined above is based on the role and context of an organisation within the IoT ecosystem. This is done based on answers to the following four categories of questions listed below:

1. Identification:

- Which LSP do you identify yourself in?

i. ACTIVAGE
ii. IoF2020
iii. MONICA
iv. SYNCHRONICITY
v. AUTOPILOT

2. Persona:

- In what context does your persona act?
  i. Demand side *[tick the box]*
     a. End-user
     b. Customer
     c. BOTH
  ii. Provider *[tick the box]*
     a. Data
     b. Services
     c. Software
     d. Hardware
     e. Network
     f. ALL

3. Data:

- What data classes are you involved in?

i. Non-Personal data
ii. Personal data
iii. Sensitive data
iv. Classified data
v. Trade Secrets & IPR
vi. ALL

4. Data Life Cycle:

- Which data life cycle phases are most relevant for you?

i. Obtain / Collect
ii. Create / Derive
iii. Use
iv. Store
v. Share / Disclose
vi. Archive
vii. Destroy / Delete
viii. ALL

Applicable Guidelines

Based on specific answers provided to the questions above, this section consists of the set of SOTA principles applicable to the respective scenario.

Please note that for purposes of this demonstration, this document only identifies the selection of relevant principles from a total of 52 principles identified reports of two workshops organised in 2016 and 2017 by the European Commission and the Alliance for Internet of Things Innovation[142],[143].

1. **User/Human factor**

1.1. **Basic principles:**

1.1.1. *Human centred approach:* Security and privacy should be universally applied to all users.

1.1.2. *Privacy by design:* Privacy of users must be embedded into the design of business processes, technologies, operations and information architectures. Each service or business process designed to use personal data must take all the necessary security requirements into consideration at the initial stages of their developments. Privacy must be embedded into the design of business processes, technologies, operations and information architectures.

1.1.3. *Privacy by default:* The strictest privacy settings and mechanisms must automatically apply once a user acquires a new product or service; no manual change to the privacy settings should be required on the part of the user.

1.1.4. *Decoupling multiple identities:* It should be easy to decouple multiple personae of the users from one another.

1.2. **User's awareness and control:**

1.2.1. *Transparency of data processing:* The service provider should empower users to know what the devices are doing and what personal data they are sharing and why, even if it concerns M2M communications and transactions.

1.2.2. *Transparency of privacy policy:* The service provider should ensure that the user is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.

1.3. **Handling of personal data:**

1.3.1. *Non-discriminatory practices:* The service provider should ensure non-discriminatory practices against users and businesses on the basis of information derived from IoT deployments (e.g. within smart cities).

1.3.2. *Manufacturer-implemented parametrization:* By design, the user should be able to configure and manage rights for accessing data controlled by them based on the assessment where (in its lifecycle) the device comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.

2. **Data**

2.1. **Data segmentation and classification:** According to the Cloud Service Level Agreement Standardisation Guidelines published by the European Commission,

[142] AIOTI. Report on Workshop on Security and Privacy in the Hyper-Connected World. <https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf>

[143] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.

"data" implies "data of any form, nature or structure, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine readable data." Service providers should ensure segmentation and classification of data that is contextualising data with respect to its purpose, risk and impact, and persona. Data classification enables processing of data with respect to the description of different classes of data. For instance, regarding personal data, data should be segmented according to the multiple personae each user has, and the related protection – including fundamental and consumer rights – it has.

2.2. **Indication of purpose:** The service provider should indicate the purpose of data collection and ensure that personal data is collected for that specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.

2.3. **Consent:** Based on the particulars provided by the data controller to the user, the user should express an informed and unambiguous consent per contextual processing of personal data (which data for which use). No data should be collected and processed without this consent.

2.4. **Data minimisation:** The less data an actor can access, the less risk there is of a security breach. If data is minimised based on a specific purpose, there is less chance that the actor will breach trust (and the law). Data minimisation starts with only requesting, collecting, obtaining, deriving and processing personal data to the extent necessary (need-to-know principle). The data provider should observe the principle of data minimisation, i.e. (i) only collect personal data whose collection the user has consented to, and (ii) erase personal data from whenever they are stored as soon as they are no longer necessary.

2.5. **De-identification:** The service provider should design and apply and de identification capabilities so personal data is de identified as soon as legally possible.

2.6. **Data control:** User should have the possibility to opt-out, right to their data, portability of their data, communication platform to control data access and to ensure security and privacy, and the overall securing of personal data processed, also in the context of related systems and devices.

2.7. **Data access:** The service provider should make it possible to technically regulate access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored (relevant in e.g. connected automobiles domain).

2.8. **Data ownership:** The service provider should clarify the principles of ownership of user's data.

2.9. **Data management/Data stewardship:** The service provider should apply a process to manage data of users not only as a business necessity but also on behalf of the individuals themselves. The service providers should apply an ethical approach to data handling.

2.10. **Data isolation:** Functional separation of datasets and databases should be in place.

2.11. **Security of personal data:** The service provider should obey by the principles of data availability, integrity, confidentiality, transparency, unlinkability/isolation and intervenability.

2.12. **Encryption:**

2.12.1. *Encryption by default:* Encryption should be applied at all stages of handling data, including in communication, storage od data at rest, storage of keys, identification, access, as well as for secure boot process.

2.12.2. *Encryption at the application layer:* Data should be encrypted on the application layer. End-to-End security, cryptographic principles and key management are extremely important and should be carefully described.

2.12.3. *Standardisation:* All aspects of cryptographic principles and key management should be carefully described.

2.13. **Compliance with data protection legislation:** Any service provider should be accountable for regulatory, contractual and ethical compliance.

2.14. **Accountability:** Any service provider should be accountable for regulatory, contractual and ethical compliance, as well as for any misuse of collected personal data. If data is compromised, disclosed, accessed or lost, clear statement by vendors, data controllers and data processors on impact is another prerequisite.

2.15. **Risk impact assessment by design:** The service provider should carry out an assessment of the risk of data being compromised, disclosed, accessed or lost. Likewise, an assessment of the consequences from regulatory, contractual and ethical perspective should be carried out.

2.15.1. *Accountability:* Any service provider should be accountable for regulatory, contractual and ethical compliance.

3. Services

3.1. **Metrics:** The service provider should engage dynamic trust key performance indicators and metrics on security, privacy, safety, resilience, reliability and the like.

3.2. **Lifetime protection:** Give security, safety and privacy protection over the full lifetime.

3.3. **Single point of contact:** The service provider should provide a single point of contact for personal data protection and privacy.

3.4. **Support:** End of support: Where the current practice is about 12 to 15 years, the end of life cycle and the related support is prerequisite. Questions to be addressed are: what happens if a services agreement is lawfully terminated, is there an update possibility, when will updating and upgrading become limited, and who is accountable for the risk of not updating IoT devices and systems.

4. Software/Application

4.1. **Security by default:** The service provider should ensure that the most secure, proven, well understood and securely updateable setting are indispensable before starting operations and during IoT life time.

4.2. **Updatability:**

4.2.1. *Secure updates:* Trusted and transparent updates should only be provided by authorised parties, not by malicious actors.

4.2.2. *Frequency of updates:* Software providers should ensure regular updates and upgrades during the device lifetime.

4.3. **Accountability and liability:** Manufacturers must be accountable and liable as they have or should have total control of the entire design, manufacturing and software development lifecycle; to execute third-party software the manufacturer should set the rules to ensure that the software is compliant with them.

4.4. **Third-party libraries:** Software developers should put rules in place for maintaining, updates and checking for vulnerabilities of third-party libraries.

5. Hardware

5.1. **Security principles:**

5.1.1. *High-level baseline:* High level baseline should be applied when safety is at stake or critical infrastructure or national safety can be materially impacted.

5.1.2. *Safe and secure interactions:* Manufacturers have to implement and validate safety principles, separately from security principles.

5.1.3. *Security rationale:* Manufacturers should be required to provide explanation of implemented security measures related to expected security risks from any designer of IoT device, auditable by independent third party.

5.1.4. *Security evaluation:* Manufacturers should specify precisely capabilities of device of a particular type. This could help to manage liability on system level.

5.1.5. *Security levels:* The industry should make use of the security scale 0 – 4 fit to the market understanding.

5.1.6. *Sustainability:* Manufacturers should ensure that connected devices as well as any IoT component as defined above are durable and maintained as per its purpose, context and respective life cycle.

5.1.7. *'As-if' by design:* The devices and ecosystems must be engineered as if these will (now or in a later phase) process personal data.

5.1.8. *Assurance:* Component and system suppliers need to be prepared for security monitoring and system maintenance over the entire life cycle and need to provide end of life guarantees for vulnerabilities notifications, updates, patches and support.

5.2. **Certification and Labelling:**

5.2.1. *Certification:* Device manufacturers should test devices and make use of existing, proven certifications recognized as state-of-the-art based on assessed risk level. Additional introduction of a classification system to certify devices for use in particular use case scenarios depending on the level of risk should be encouraged.

5.2.2. *Trusted IoT label:* Labels such as the 'Energy efficiency label' of appliances should give a baseline requirement of protection based on the level of assurances and robustness and should be used to classify individual IoT devices.

5.3. **Secure Performance and Functionality:**

5.3.1. *Defined functions:* Manufacturers should ensure that IoT devices are only able to perform documented functions, particular for the device/service.

5.3.2. *Secure interface points:* Manufacturers should identify and secure interface points also to reduce the risk of security breach.

6. Authentication

6.1. **Authentication of identities among themselves:** In the context of communication of various applications, authentication of identities should be open to all technologies and applications.

6.2. **Identity protection by design:** Decoupling personal identity of a user from device identity should be possible.

6.3. **Transparent roles:** The service provider should ensure clear allocation and identification of roles, including who is data controller, co-controller, processor, co-processor, and so forth.

7. Infrastructure/Network

7.1. **Architecture & Ecosystem:**

7.1.1. *Interoperability:* Stakeholders should aim at achieving interoperability of components and communication protocols. Manufacturers should aim at creating interoperable devices.

7.2. **Knowledge sharing:**

7.2.1. *Monitor and respond:* Stakeholders should ensure continuous monitoring and improvement of relevant IoT ecosystems, including clear metrics and measurements.

7.2.2. *Information sharing platforms:* Stakeholders should be active in sharing information about incidents/potential vulnerabilities with each other.

Other items

1. **Independent privacy and security audits:** Organizations of certain size and public bodies should mandatorily carry out third party privacy and security audits.
2. **Harmonised industry approach:** Stakeholders should participate in standardisation efforts of the functional and security assurance requirements through common harmonised industry approach. This should ensure that devices are designed, manufactured and assembled with clear understanding of what means what, and to what extent there is consensus in the related complex value chain and ecosystems. At the same time, the goals of data protection such as limiting the scope of data processing to the necessary level should be promoted, as well as data segmentation, mapping, categorisation, purpose limitation, data isolation, and data control and data access of personal data are seen as prerequisite elements.
3. **Reduce impact of national regulations:** Stakeholders should actively participate in harmonisation efforts to reduce the impact of different national regulations.
4. **Taxonomy:** The basic taxonomy does not need to be perfect, but sufficiently workable. Definitions established as prerequisite include *data*, *personal data*, *data controllers and other actors*, *the personal data life cycle*, *IoT ecosystems* and the *physical* and *virtual "Things"*.

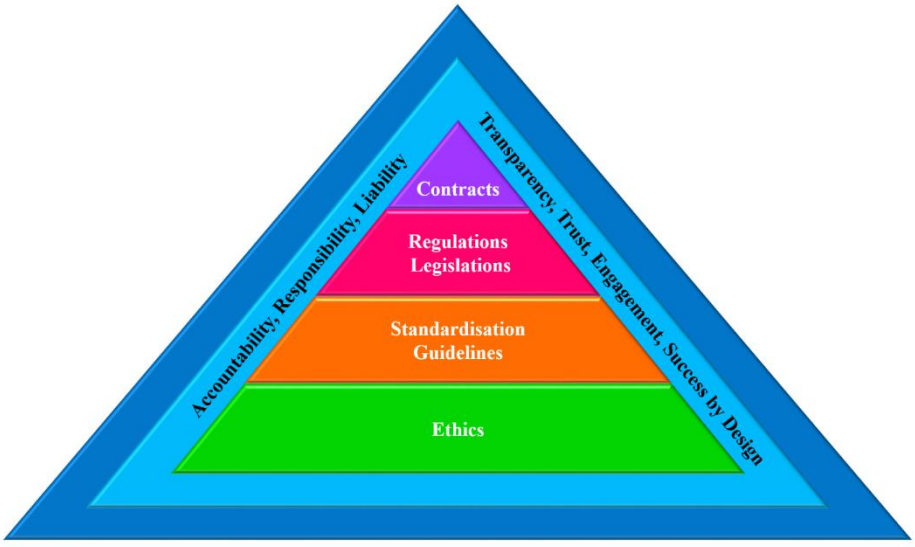
Code of IoT Engagement

1. WHY THIS CODE?

Imagine you want to be part of a sports team, a musical ensemble, an innovation hub, a rural or urban area or even a country. With that, you want to become part of a certain community, each with its particular habits, codes and rules. These are meant to set the expectations of the members of such community straight, and meanwhile protect the interests of each of them separately, the community as a whole, as well as society and its environment.

Welcome to the world of IoT and the European Large-Scale Pilots Programme, where you and your community can be part of, connect with new people, things and other opportunities, engage, test, try, pivot, iterate, hyper-connect, calibrate, collaborate, mature, mitigate risks, optimize results and succeed. We call this Success by Design.

In order to organise this, and – again – to set the expectations straight and aim to avoid discussions and conflicts, we need to play by some rules. The framework of those rules are in this Code of IoT Engagement.



In the era of the technological galloping – which we embrace but also try to understand and where necessary organise and mitigate risk and negative impacts – we are all experiencing, human knowledge and experience on given concepts are challenged. In the Internet of Things era, the very essence of the notion of knowledge and experience is challenged.

Bearing in mind this very interesting challenge and its vast amount of various opportunities, this Code of IoT Engagement is meant to navigate, enable and facilitate pleasant, fair, reasonable, highly-ethical and successful engagement between you and the relevant members and domains of the communities and IoT ecosystems within the European Large-Scale Pilots Programme.

This code will demystify engagement in the IoT context and shed light on the very grounds of this engagement.

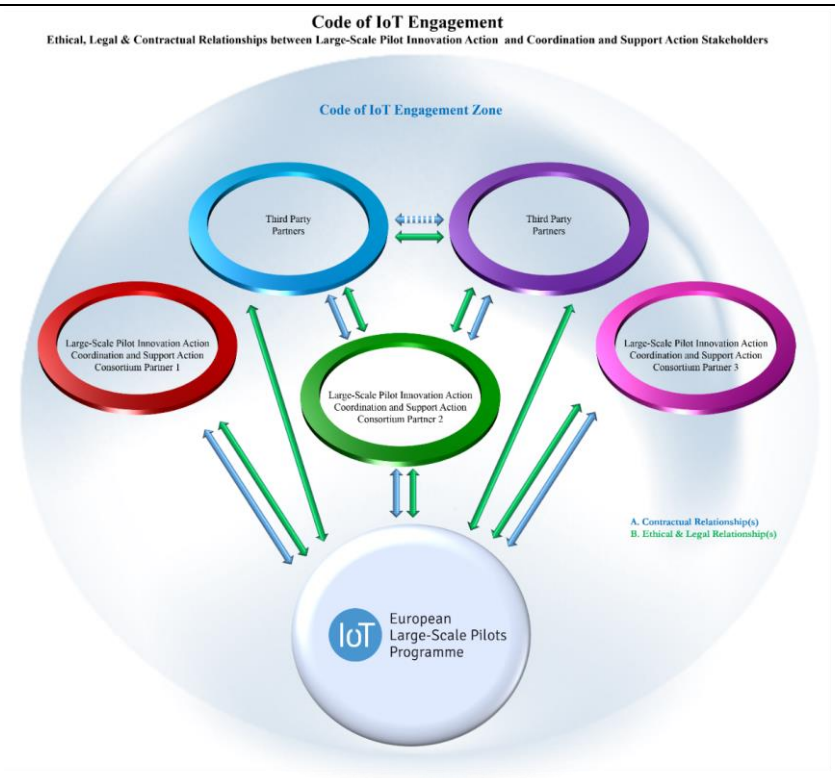
2. WHO IS WHO?

This Code of IoT Engagements ('Code') is applicable to each and every one – and everything – that in anyway wish to become part of any part of a community, ecosystem within the vast domains of the Large-Scale Pilots (LSPs) and Coordination and Support Activities (CSAs) of the European Large-Scale Pilots Programme. It is not only good to understand who you are within those domains but also who the other stakeholders maybe you will or may engage with.

These include, without limitation the following stakeholders, in random order:

a. Society and environment
b. Users
c. Users
d. Customers
e. Non-users
f. Data brokers
g. Data providers
h. Service providers
i. Software providers
j. Hardware providers
k. Infrastructure providers
l. Machines, interfaces and user-interfaces
m. Universities and other knowledge institutions
n. Standardisation development organisations
o. Policy makers: governments, municipalities and others
p. Authorities, law enforcement and intelligence services

The figure below illustrates how these stakeholders relate to each other, where for instance parties that are not part of a LSP or CSA consortium are indicated as Third-Party Partners or Third-Party Suppliers. They engage with a specific LSP or CSA consortium partner though this Code and with that are engaged with them within the European Large-Scale Pilots Programme.



3. DECLARATION OF ADHERENCE

I hereby declare that I adhere to the Code of IoT Engagement.

4. BACKGROUND INFORMATION

The latest technological developments have surfaced in an unprecedented manner the insufficiencies of the existing laws to tackle with a series of matters of paramount significance both for individuals and society at large. The expansion of the internet of things, the galloping of artificial intelligence, the widespread use of drones, are merely an indicative list of examples triggering questions around human autonomy, the extent of human decision making or even the scope of fundamental human rights. Taking into account those concerns, the present document produced by CREATE-IoT project discusses how the ongoing European large-scale pilots programme can be legally compliant, while meeting the criteria of an ethical assessment as set forth by the European Commission[144].

Naturally, the development of technology and responding to the needs of the future dynamic IoT systems, which is at the core of CREATE-IoT large scale pilots (LSPs), has to be carried out in compliance with statutory (legal) requirements. However, since legal compliance may in some instances fall short of observing core ethical principles, supplementary ethical requirements have to be provided in this code of IoT engagement.

Overall, though, LSPs are expected to comply with a complex set of requirements stemming from different sources, as illustrated in the figure below:

This set of requirements creates a load of obligations for the LSPs that may vary significantly depending on the exact role of each organisation with a role within the IoT LSP consortium. Bearing in mind this complexity, the present code of IoT engagement will demystify the scene

[144] H2020 Programme Guidance 'How to complete your ethics self-assessment', available at: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

aiming to ensure that each LSP as a whole, as well as, each organization being part of each LSP is compliant with the relevant set of rules dictating their responsibilities under law and ethics.

Based on this code of IoT engagement LSPs will be in the position to assess themselves what is permissible and what is not with respect to privacy and security in the IoT environment.

Distinction between code of ethics and code of conduct; distinctive elements of the concept – and a value- of a Code of an IoT Engagement.

5. LIFECYCLE THINKING

IoT is a dynamic living system, not static, therefore, allowing for an approach on the basis of separate lifecycles

IoT Device/Product Life Cycle: What does the life cycle entails, how long needs and can a device/product remain connected to an IoT ecosystem in a secure, safe and compliant manner, what can the user/customer expect, and how is both the device/product as well as the user/customer able to keep up to date with (at least) the state of practice?

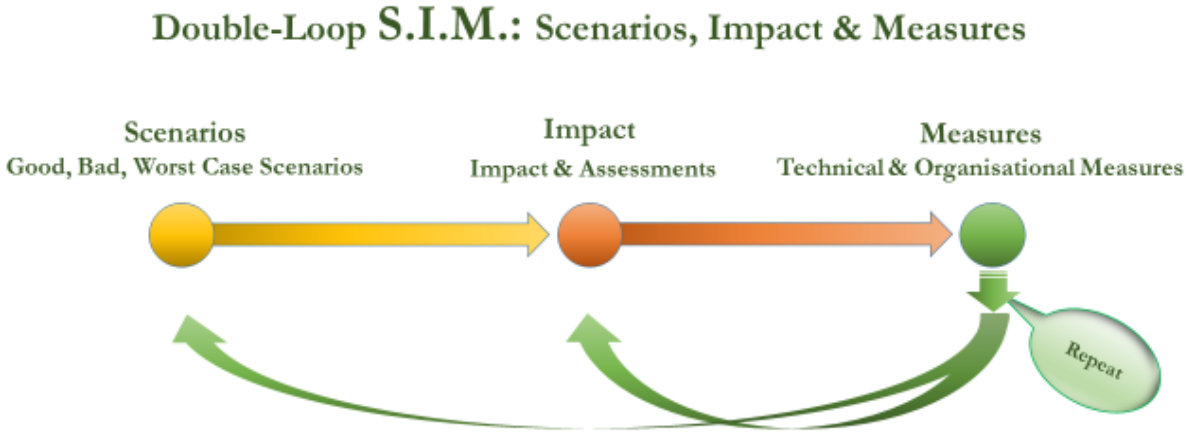
Stakeholders Life Cycle: What stakeholders are involved regarding an IoT device/product and in a relevant IoT ecosystem, what if the dynamics thereof changes, who is accountable for what part of the ecosystem, how to keep the stakeholders up to date, and what happens if there is an incident of any kind within the IoT ecosystem?

Data Life Cycle: What data is collected, created or otherwise concerned, what is its classification, can it be segmented, minimised and isolated, what if it has multiple classifications and what if the classification changes, how controls the data, for what purposes is one entitled to process the data, what meta data and derived data is generated during the data life cycle, and what does data deletion mean?

Contextual Life Cycle: In what context is a device/product/ecosystem used, as what persona is a stakeholder involved and in what context is data used in an IoT ecosystem, what if the context thereof changes, who is accountable in what context, how to make stakeholders aware of changes in best practices, rights and obligations when the context changes, and how to secure the rights and obligations of the relevant other stakeholders?

Legal Life Cycle: As a person or legal entity, with whom do you want to engage? And if so, how to assess, prepare, negotiate, contract, execute, operate, update, amend, escalate and terminate such engagement (a.k.a. legal relationship)?

Double Looping



6. APPLICABLE REGULATION

6.1. 2012/C 326/02: Charter of Fundamental Rights of the European Union

6.1.1. *Article 1 – Human dignity:* Human dignity is inviolable. It must be respected and protected.

6.1.2. *Article 7 – Respect for private and family life:* Everyone has the right to respect for his or her private and family life, home and communications.

6.1.3. *Article 8 – Protection of personal data:* (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.

6.1.4. *Article 21 – Non-discrimination:* Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

6.2. Regulation (EU) 2016/679: General Data Protection Regulation

6.2.1. *Article 5 – Principles relating to processing of personal data*

6.2.2. *Article 9 – Processing of special categories of personal data*

6.3. Directive (EU) 2016/1148: NIS Directive

6.3.1. *Article 2 – Processing of personal data*

6.4. Directive 2002/58/EC: e-Privacy Directive

6.4.1. *Article 4 – Security:* (1) the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary, in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. (2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

6.4.2. *Article 5 – Confidentiality of the communications:* (1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). (...) (3) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia

about the purposes of the processing, and is offered the right to refuse such processing by the data controller. (...)

6.4.3. *Article 6 – Traffic data:* (1) Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). (...) (3) For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. (4) The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3. (...)

6.4.4. *Article 7 – Itemised billing:* (1) Subscribers shall have the right to receive non-itemised bills. (...)

6.4.5. *Article 9 – Location data other than traffic data:* (1) Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. (2) Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. (3) Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

6.4.6. *Article 12 – Directories of subscribers:* Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. (...)

6.5. **Regulation (EU) No 1291/2013: Establishing Horizon 2020**

6.5.1. *Article 16: Gender equality*

6.5.2. *Article 18: Open access*

6.5.3. *Article 19: Ethical principles*: Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection.

6.6. **H2020 Programme Guidance: How to complete your ethics self-assessment**

6.7. **Council Regulation (EC) No 338/97: Protection of species of wild fauna and flora**

6.8. **Directive 2009/41/EC: Contained use of genetically modified micro-organisms:** The Directive concerns Members States' obligation to take appropriate steps to avoid adverse effects on human health and the environment which might arise from the contained use of GMMs.

6.9. **Directive 2006/25/EC: Minimum health and safety requirements of workers**

6.10. **Regulation No 428/2009: Handling dual-use items**

7. ACCOUNTABILITY

Who is responsible for the enforcement of this code?

8. CONSEQUENCES OF NON-ADHERENCE & NON-COMPIANCE

What happens in case of non-compliance? Are there remedies in place?

9. APPENDICES

APPENDIX I- ETHICAL PRINCIPLES

This Section presents the ethical principles to be observed by all participants taking part in CREATE-IoT LSPs. Reference to Article Human dignity is inviolable. It must be respected and protected.'

- Article 1,EU Charter of Fundamental Rights

To ensure consistency and clarity, some key general ethical principles are summarised in points a. to i. below:

a. **Human dignity** is inviolable. It must be respected and protected.

b. Any practices engaged must adhere to the principles of **freedom**, **security and justice economic and social progress**, and to the **well-being of natural persons**.

c. **Discriminatory practices** and discriminatory treatment must be avoided.

d. Special care must be taken in cases of **minors, special groups and vulnerable individuals**.

e. **Personal data** remains ownership of individuals and may not be collected and/or handled without a freely given, specific, informed and unambiguous consent. Protection of natural persons in relation to the processing of personal data remains a fundamental right, however, not an absolute right. Data subject's right of access to personal data as well as right to be forgotten must be observed.

f. **Transparency:** Data subjects must be informed about the types and volume of data to be stored as well as about any transmission of their data to third parties. The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be

used.

g. **Accountability:** It must be possible to establish what an entity did at any point in the past and how.

h. **Technological neutrality:** These ethical principles apply universally, regardless of technology, technological means of carrying out a (research) project or technological means of handling personal data.

i. **Ethics board** or **ethics advisor** must be appointed which includes relevant independent expertise to monitor, endorse and oversee the implementation of ethical concerns in any project.

Sections 9.1 to 9.3 outline numerous domain-specific ethical principles:

9.1. **Personal data[145]:**

9.1.1. *Ownership:* Personal data remains ownership of the data subject.

9.1.2. *Collection only with consent:* Personal data can only be collected from consenting data subjects. They possess independent capacity to clearly understand what the process entails and agree to it. Consent must be informed as well as explicit and affirmative, i.e. expressed through a clear agreement to stated terms. Personal data will not be collected from a non-consenting data subject.

9.1.3. *Obtaining consent:* Consents have to be handled through the user interface allowing the data subjects to agree the transmission and storage of sensitive data. The consent legal text must be customized for each country where the controller is seeking consent from data subjects, with respect to applicable local legislation.

9.1.4. *Notification:* Data subjects must be notified that their data is being collected and about how this data will be disclosed and used. This notice must be provided in and easily located and readily accessible format.

9.1.5. *Justification for collection:* Justification must be given in case of collection and/or processing of personal sensitive data.

9.1.6. *Purpose specification and limitation:* The consent text included in the interface should specify which data will be stored, who it will be transmitted to and for which purpose. Personal data may only be collected for the specified purpose and not further processed in a way incompatible with the stated purpose.

9.1.7. *Terms and definitions:* Data subjects should know with whom they are contracting, if the contract involves sharing with third parties, partners, business partners, the controller's partners, or affiliates. Controllers should clearly explain the following definitions in a consistent manner in all of their respective agreements: (1) data; (2) third party; (3) partner; (4) business partner; (5) controller's partners; (6) affiliate; (7) data account holder; (8) original data subject data. If these definitions are not used, the controller should define each alternative term in the contract and privacy policy. Controllers should strive to use clear language for their terms, conditions and agreements.

9.1.8. *Information on procedures:* Detailed information must be provided on the procedures that will be implemented for data collection, storage, protection,

[145] Relevant for ACTIVAGE, SYNCHRONICITY, MONICA and AUTOPILOT. Source: GDPR.

retention, transfer, and destruction or re-use and confirmation that they comply with national and EU legislation.

9.1.9. *Information on informed consent:* Detailed information on the informed consent procedures that will be implemented in regard to the collection, storage and protection of personal data must be submitted on request.

9.1.10. *Consent forms and information sheets:* Templates of the informed consent forms and information sheet must be submitted on request.

9.1.11. *Public availability of data:* A controller using public available personal data must explicitly confirm that the data used is publicly available.

9.1.12. *Unnecessary collection:* A controller must clarify which personal data will be collected from data subjects and confirm that they will avoid and prevent any unnecessary collection and use of data.

9.1.13. *Sensitive data, genetic information, tracking:* If the (research) activity involves the collection or processing of sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction), genetic information or tracking of participants, the necessary notification or authorization for processing of this data must be obtained (if required).

9.1.14. *Anonymity:* The anonymous participation of citizens to the proceeding shall be enabled for those countries whose legislation explicitly defines this right.

9.1.15. *Minimization:* Only the amount of personal data needed for the operational purposes of the project should be collected.

9.1.16. *Transparency:* Data subjects must be informed about the type and volume of data to be stored, how it will be transmitted, at what locations and for which purposes must be openly communicated to all participants within and outside a consortium, including consenting participants volunteering their private data. Data subjects must also be informed about how they can contact the controller with inquiries or complaints, the types of third parties to which the controllers disclose the data and options the controller offers for limiting use and disclosure. Controllers' principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts. A controller should not change the contract with the data subject without their agreement.

9.1.17. *No data sharing by default:* By default, personal data is not automatically shared. Data sharing and diffusion only applies to data for which consent has been given, and in accordance with the diffusion terms expressed by the consent.

9.1.18. *Data retention, availability and erasure:* Personal data cannot be stored longer than needed for specific and clearly defined purposes and must be in a format that allows its erasure or anonymization. Each controller should provide for the removal, secure destruction and return of original data subject's data from the data subject's account upon the request of the data subject or after a pre-agreed period of time. The controller should include a requirement that data subjects have access to the data that a controller holds during that data retention period. Controllers should document personally identifiable data retention and availability policies and disposal procedures and specify requirements of data under policies and procedures.

9.1.19. *Cookies:* The system shall not store cookies on the data subjects' computers to

prevent any unauthorized tracking of the data subjects' activities on the Internet.

9.1.20. *Data safety:* Details must be provided on data safety procedures (protective measures to avoid unforeseen usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources).

9.1.21. *Encryption:* Encryption will be applied to personal data when in transit and when at rest. State-of-the-art encryption technology must be applied for all data exchange within the project: e.g. SSL, TLS.

9.1.22. *Hosting of Data:* All personal data must be stored on a verified secure server, preferably within the country from which it was collected.

9.1.23. *Disclosure, use and sale limitation:* A controller will not sell and/or disclose non-aggregated data subject's data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions as the controller has with the data subject. Data subjects must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale. A controller will not share or disclose original data subject's data with a third party in any manner that is inconsistent with the contract with the controller. If the agreement with the third party is not the same as the agreement with the controller, controllers must be presented with the third party's terms for agreement or rejection.

9.1.24. *Right of access:* Data subjects should have a right of access to personal data which have been collected concerning them, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

9.1.25. *Contract termination:* Data subjects should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations. Procedures for termination of services should be clearly defined in the contract.

9.1.26. *Unlawful or anti-competitive activities:* Controllers should not use the data for unlawful or anti-competitive activities, such as a prohibition on the use of data subject's data by the controller to speculate in commodity markets.

9.1.27. *Liability and security safeguards:* The controller should clearly define terms of liability. Data subject's data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. Polices for notification and response in the event of a breach should be established.

9.1.28. *Secondary use:* If research involves further processing of previously collected personal data, the controller must provide details on the database used or of the source of the data, details of procedures for data processing, details of data safety procedures, confirmation that data is openly and publicly accessible or that consent for secondary use has been obtained, confirmation permissions by the owner of the data sets.

9.2. **Animals[146]:**

9.2.1. *Involvement of animals:* If the (research) activity involves animals, the

[146] Relevant for IoF2020.

controller must provide details of species and rationale for their use, numbers of animals to be used, nature of the experiments, procedures and techniques to be used. The controller should also provide justification of animal use (including the kind of animals to be used) and why alternatives cannot be used.

9.2.2. *Special groups:* Additional information must be provided in cases of the following special groups:

9.2.2.1. Non-human primates (NHP): Explanation of why are NHPs the only research subjects suitable for achieving the scientific objectives. Details of the purpose of the animal testing. Details of the animals' origin. Provide personal history file of NHP.

9.2.2.2. Genetically modified animals: Details of the phenotype and any inherent suffering expected. Details of the scientific justification present for producing such animals. Details on the measures to be taken to minimise suffering in breeding, maintaining the colony and using the GM animals. Provide copies of GMO authorisations.

9.2.2.3. Cloned farm animals: Details of the phenotype and any inherent suffering expected. Details on the scientific justification for producing such animals. Details on the measures taken to minimise suffering in breeding, maintaining the colony and using of the GM animals. Provide copies of authorisations for cloning (if required).

9.2.2.4. Endangered species: Give details on why there is no alternative to using this species. Give details on the purpose of the research. Provide copies of authorisations for supply of endangered animal species (including CITES).

9.2.3. *RRR:* Implement the principles of Replacement, Reduction and Refinement where possible. Replacement — replacing animal use by an alternative method or testing strategy (without use of live animals). Reduction — reducing the number of animals used. Refinement — improving the breeding, accommodation and care of animals and the methods used to minimise pain, suffering, distress or lasting harm to animals.

9.2.4. *Authorisation:* Obtain authorisations for the supply of animals and the animal experiments (and other specific authorisations, if applicable).

9.3. **Environment, Health & Society[147]:**

9.3.1. *Possible harm to environment:* Further information about the possible harm to the environment caused by the (research) activity must be provided as well as the measures that will be taken to mitigate the risks, including risks due to underestimated methodological limitations or reliance on datasets of poor quality or reliability.

9.3.2. *Health and safety:* The applicant is required to apply the precautionary principle where there is plausible scientific evidence for serious risks and provide details on health and safety measures to be implemented.

9.3.3. *Use of harmful elements (humans):* Specify whether the (research) activities involve the use of elements that may cause harm to humans including research

[147] Relevant for SYNCHRONICITY, IoF2020 and AUTOPILOT.

staff. Specify the nature of health and safety procedures applied.

9.3.4. *Use of harmful elements (environment):* Specify whether the (research) activities involve the use of elements capable of causing harm to the environment, animals or plants. Provide risk-benefit analysis. Show that the researcher applies the precautionary principle. Specify what safety measures will be taken.

9.3.5. *Endangered areas:* Specify whether the research will deal with endangered fauna and/or flora and/or protected areas.

APPENDIX II: DEFINITIONS[148]

1. **Personal data** means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR)
2. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (GDPR)
3. **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (GDPR)
4. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. (GDPR)
5. **Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. (GDPR)
6. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (GDPR)
7. **Processor means** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. (GDPR)

[148] Further relevant definitions can be found in the text of the General Data Protection Regulation (GDPR)