CREATE-IoT

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

European Large-Scale Pilots Programme

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.08

IoT Policy Framework Common Event

Revision: 1.00
Due date: 30-04-2020 (m40)
Actual submission date: 30-04-2020
Lead partner: SINTEF

European Commission

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	**D05.08 IoT Policy Framework Common Event**				
Status	Released	**Due**	m40	**Date**	30-04-2020
Author(s)	O. Vermesan (SINTEF), R. Bahr (SINTEF), J. Gato (ATOS), R. Little (ATOS), Sébastien Ziegler (MI), P. Annicchino (AS), A. Tringale (ISMB)				
Editor	O. Vermesan (SINTEF)				
DoW	Common event with the IoT Large-Scale Pilots (LSPs) for aligning the IoT policy framework and discuss the recommendations. The work is part of task T05.01 (Policy framework and trusted IoT environment). The present document presents the relevant information in addition to the summary of the common event organised with the LSPs.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	26-01-2019	SINTEF	Template.
0.01	26-11-2019	SINTEF	Initial version.
0.02	21-02-2019	SINTEF	Structure and ToC.
0.03	01-04-2019	AS	Initial draft and contribution.
0.04	20-04-2019	SINTEF	The LSPs contribution regarding IoT Security, Privacy and Trust.
0.05	21-04-2019	SINTEF	AUTOPILOT update.
0.06	23-04-2019	AL	Review comments.
0.07	24-04-2019	ATOS	Input and comments.
0.08	28-04-2019	ISMB	Input and comments from MONICA.
0.09	30-04-2019	SINTEF	Review comments considered.
1.00	30-04-2019	SINTEF	Final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Publishable summary

The IoT Policy Framework Common Event organized by CREATE-IoT on 20th of February 2020, in the context of the *Navigating IoT Architectures and Standard Days* which took place in Brussels at DG Connect 19th to 21st February 2020. Based on the IoT policy framework in WP05 and deliverable D05.01, the event provided an opportunity to discuss IoT Security, privacy policy framework and elaborate on the strategy taken by the LSPs.

The event offered to the participants the opportunity to understand the security and privacy requirements strategies, identify existing best practices and ways forward and reflect on the new digital strategy finalized by the European Commission which will have an important impact on the IoT ecosystem and policy framework. Many of the participants attended the ETSI STF547 Public Dissemination Workshop and had the opportunity to exchange their views on the outcome of the ETSI Specialist Task Force (STF) 547 related to security, privacy, and trust.

The discussions have focused on LSPSs experience built-up, best practices, main activities, while answering the following questions:

- What were the main drivers in the LSPs domain/use cases for security and privacy?
- How LSPs addressed cybersecurity requirements in the system architecture/operational setup for the pilots? How LSPs tackled the GDPR (General Data Protection Regulation) compliance?
- What were the main challenges to address the requirements in the pilots? Have the LSP performed a detailed risk/vulnerability and impact analysis?
- What are the major future technical solutions that LSPs are using/needed to effectively address IoT security and privacy by design?
- Based on the experience in the implementations, have the LSPs identified a need for regulators intervention to harmonise requirements/practices and build a level playing field in those areas?

1.2 Non-publishable information

The document is public.

2. INTRODUCTION

2.1 Purpose and target group

The successful development and deployment of IoT solutions relies on multi-dimensional IoT reference architectures that address the different functional layers, the cross-cutting functions and system properties. These include the requirements for device security, device discovery, provisioning and management, data normalization, analytics, and services.

The IoT reference architectures are key for standardization. They define guidelines that can be used when planning the implementation of IoT systems, in order to address the complexity of IoT solutions, and ensure trustworthy, secure scalable, and interoperable IoT deployments.

The event has included discussions bringing answers to what has been achieved and what remains to be done by the IoT and DEI Large Scale Pilots Programme funded under Horizon 2020. With the help of the coordination and support actions CREATE-IoT, NGIoT (Next Generation Internet of Things) and OPEN-DEI (Open Platforms and Large-Scale Pilots in Digitising European Industry) these projects are expected to team up together in order to have significant contributions to piloting European platforms,

Data ecosystems, standardisation, and pre-normative activities. The event was open to the representatives of the IoT European Large-Scale Pilots Programme projects, DEI Large-Scale Pilots, AIOTI members and SDOs contributors.

2.2 Contributions of partners

SINTEF is responsible for the common event with the IoT LSPs for aligning the IoT policy framework and discuss the recommendations. Support for 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. Describe the contribution from AUTOPILOT and alignment of activities.

ATOS has actively participated in the event and the different round tables (world café discussion). In these round tables ATOS specially contributed about Synchronicity LSP, IoT and data interoperability mechanisms (such as Marketplaces). In addition, ATOS presented the project BD4OPEM, in a session about Open DEI. The objective of presenting these projects was to establish common actions, and identify horizontal coordination, for example, about data sharing strategy. In addition, we have helped contribute to the quality of the deliverable.

MI: has presented the collaborative white paper developed by CREATE-IoT with the LSPs on lessons learned from the IoT European Large-Scale Pilots Programme projects with regards to personal data protection for IoT deployments. MI actively participated in the event and the different round tables and co-animated one of the sessions.

AS has participated to the event and worked on the initial draft of the deliverable. It has shared the initial table of contents with the partners and worked on the revision of the IoT policy framework in particular from the point of view of privacy and security. In the context of the discussions and the roundtables AS has contributed to the exchange on data protection and security, the evolution and assessment of the LSPs and standardization initiatives. It has also built on the contribution on the coordination of the two CSAs considering the work done in the context of U4IoT.

2.3 Relations to other activities in the project

This event has been organized within the framework of the activities of CREATE-IoT Work Package 5 (IoT Policy Framework- Trusted, Safe and Legal Environment for IoT). It has also benefited from the contributions stemming from on-going work in the IoT LSPs and the IoT Activity Group AG05 (IoT privacy, end-user engagement and ethics).

The workshop has been promoted through different channels such as:

- AG05 mailing list.
- CREATE-IoT and IoT LSP web site.
- IoT LSP Newsletter.
- CREATE-IoT social networks: Twitter, LindedIn and Facebook.
- Partners' social networks.

3. IoT Policy Framework - European Large-Scale Pilots Programme

This chapter gives an overview of the IoT policy framework developed by CREATE-IoT to provide the structure and a set of principles for IoT solutions that were further developed together with the LSPs to address the main components for tackling IoT trust, security, privacy and engagement.

The chapter summarises the IoT policy issues further developed by each of the 5 LSPs and summarises their contributions and achievements. This policy framework was central to discussions at the event.

3.1 The IoT Policy Framework overview

CREATE-IoT has developed an IoT Policy Framework as a conceptual structure aimed at organizing and clarifying the fundamental concepts and principles, practices and requirements surveyed thorough the work with the different LSPs and in consultation with several stakeholders.

The IoT Trust framework developed "provides an underlying structure and a set of principles that manifest trustworthiness, dependability and privacy for IoT solutions in an integrated manner" [1].

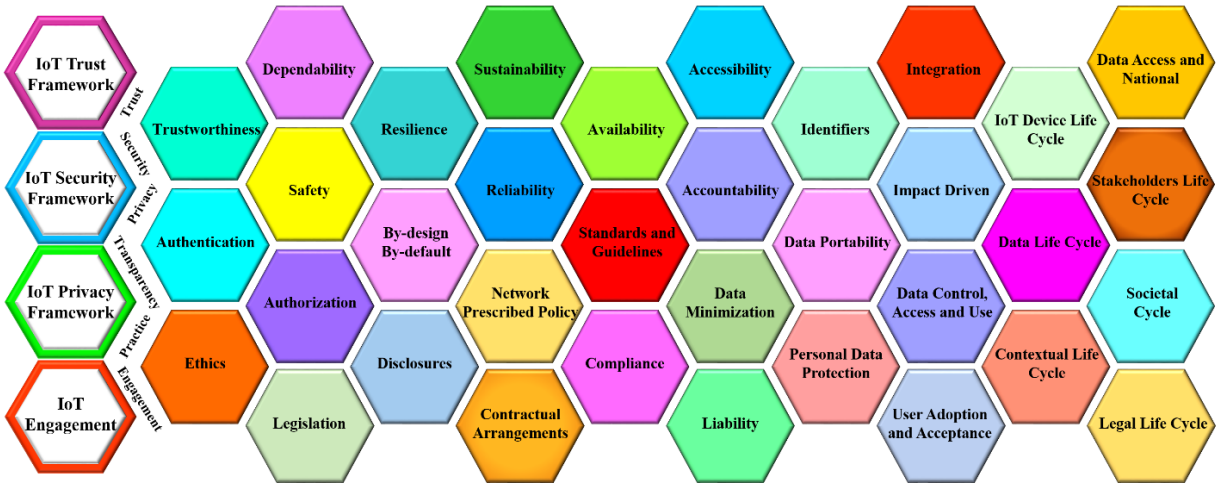

Figure 1:Constitutive elements of the IoT Policy framework [1]

3.1.1 IoT Trust Framework

The Policy framework has analysed the different dimensions and definitions of trust highlighting its central role in the development of the ecosystem. Trust must be understood in its different dimensions and perspectives:

- *Socio-economical perspective* as it is recognized that "trust enhances economic efficacy under certain conditions" [1].
- *Business perspective* as "trust in IoT is an indispensable prerequisite for the growth of IoT business" [1].

Trust therefore has come to be understood in its multiple dimensions "combining, for example, privacy, security reliability, availability, and integrity with human and machine behaviour" [1] which requires an appropriate design "remunerating the social assumptions and examining how those assumptions can function to put some users of the system at risk.

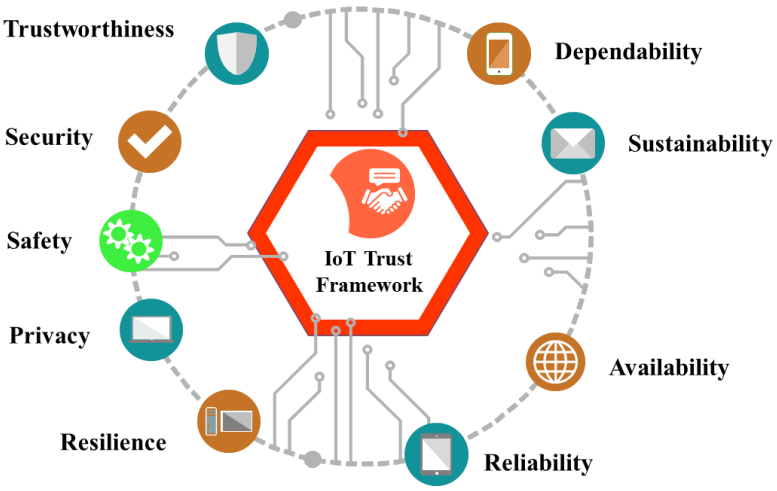

Figure 2: IoT Trust components

To understand and design trust systems requires acknowledgment of the social, human, and autonomous/cognitive elements" [1].

3.1.2 IoT Engagement Framework

The engagement framework must be understood as a core component of an IoT policy framework. The IoT engagement framework elements identified are: Ethics, Standards and Guidelines, Legislation and Contractual Agreements. Engagement is a crucial part of the building of trust with the different stakeholders and it "constitutes a quite complex objective as it presumes organizational awareness, development of an organizational culture that ensures the translation of norms and values into concrete practices, as well as, the investment of necessary resources" [1]. In this context detailed work has also being pursued in the context of CREATE-IoT cooperation with U4IoT in the context of the AG05.

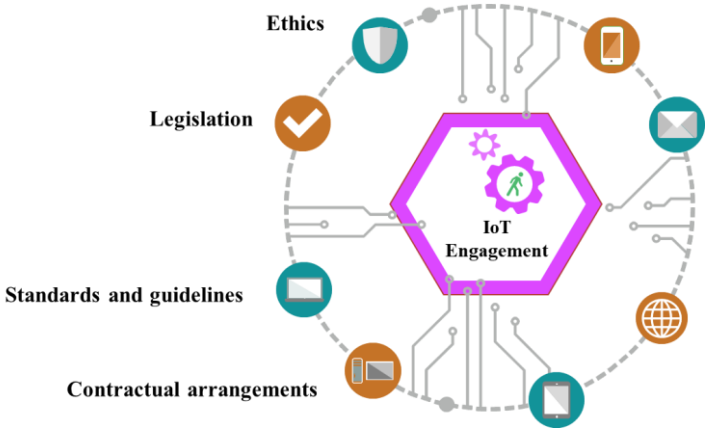

Figure 3: IoT IoT engagement framework

3.1.3 IoT Privacy Framework

Data protection and privacy are at the core of the IoT Policy framework as only an ecosystem that protects personal data and is able to extract added value from proper data management will be able to maximize the benefits of IoT deployment. As we have already underlined in deliverable 05.01: "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" [1].

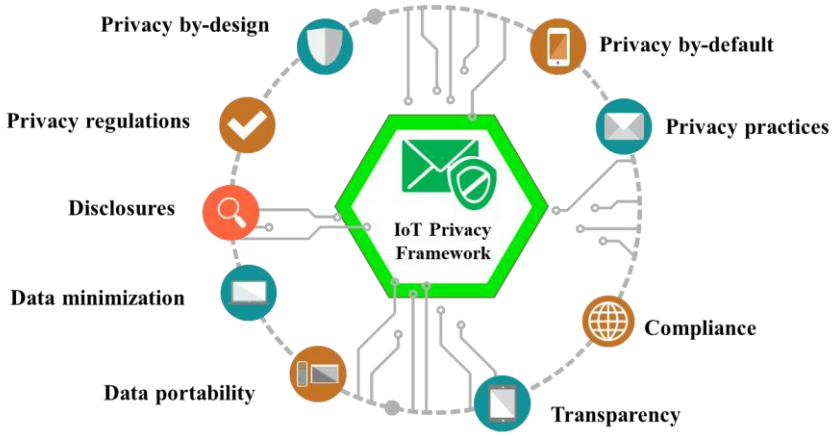

Figure 4: IoT Privacy framework

3.1.4 IoT Security Framework

The security framework is another fundamental stone of the IoT policy framework. The building blocks around which security is guaranteed are impact assessment exercises and design of controls.

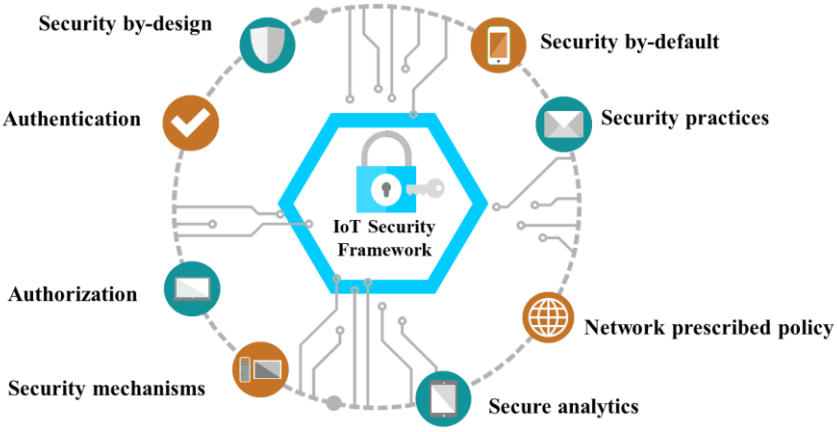

Figure 5: IoT Security Framework

The security framework considers the following elements:

- Ensuring IoT security mechanisms.
- Ensuring IoT data protection.
- Ensuring IoT system resilience.
- Providing IoT system/application trust" [1]

3.2 The LSPs contribution

During the IoT & DEI Large Scale Pilots workshops Franck Boissière (EC E4 DG Connect) highlighted how the different LSPs have contributed to the research in the IoT ecosystem. The main achievements of the projects have previously been presented and a detailed description can be found in the CREATE-IoT deliverable D06.11 [4]. The different LSPs have dealt with providing trusted solutions for IoT deployment in the different verticals and in doing so have also cooperated with the two Coordination and Support Actions (CSAs). The main lessons learned have been collected and made public through the publication of the guidelines "*Personal Data Protection for Internet of Things Deployments: Lessons Learned from the European Large-Scale Pilots of Internet of Things*" [5]. This document has been elaborated in cooperation with the LSPs and publicly discussed in several meetings, conferences, and sessions of the AG05. They have addressed their different domain-specific data protection and security requirements. For instance, ACTIVAGE developed a Security and Privacy framework based on three main

principles: privacy, trust, and security. ACTIVAGE also executed a security and privacy risk assessment. AUTOPILOT developed four frameworks for the use of autonomous vehicles augmented by IoT: a policy framework; a security framework; a privacy framework; and an engagement framework. It followed the ETSI Intelligent Transport System (ITS) for the privacy and security architecture. Several enablers have been developed in the context of the LSPs: data protection impact assessments have been executed in the context of the different projects, SYNCHRONICITY developed a dedicated Data Protection Impact Assessment for Smart-cities; it also made available a PrivacyApp to enable citizens to access information on IoT deployments in their city. In the context of SYNCHRONICITY, the "EuroPrivacy certification scheme" [21] has been extended and adapted to cover the requirements for smart cities. In the context of the LSPs various technologies for data management and data sharing have also been adopted. This has been the case for encryption and pseudonymization, semantic services, blockchain technologies. Through a survey organized by the AG05 we were able to gather more details on the activities of the different LSPs in the field.

The following sub sections present the summaries of the activities on the IoT policy framework topics performed by the IoT European Large-Scale Pilots Programme projects that were used as reference for the presentations and discussions during the event.

3.2.1 ACTIVAGE

DPIA and STRIDE Analysis and Recommendation

ACTIVAGE has developed a specific end-to-end security methodology to identify, analyse and mitigate any identified risks related to data protection and security of the deployed system. The methodology checks the deployed system by assessing the integrity, confidentiality, availability and authorization. It considers the potential impact of vulnerabilities. It also performs specific data protection impact assessment with a specific focus on: data minimization, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features.

Secured Gateway

ACTIVAGE has developed a secured gateway based on open source hardware (Raspberry PI 3). It provides strong authentication at network and application levels. This secured gateway enables higher of security and protection of any collected data and enables to filter and process part of the data at the edge.

Blockchain-based Registry

ACTIVAGE has proposed the introduction of Distributed Ledger Technologies through the implementation of a consent form mechanism and Permission handling registry leveraging blockchain technology. This Blockchain as a Service (BaaS) approach being proposed by CERTH/ITI, ensures a strong reliability of any permissions given or withdrawn by the end-user.

IoT Security, Privacy and Trust:

Analysis carried out by ACTIVAGE shows that the nature of Active and Healthy Ageing (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, and security is a continuous process with integrated improvement procedure, based on the continuous evaluation of the in-place security.

Since security is a continuous process, continuous evaluation is needed. External inspection

such as auditing is a must. Self-auditing and internal expertise are present, 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.

ACTIVAGE 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.

Security issues emerge according to IoT architecture, protocols used for networking, communication, and the overall management. Regarding trust evaluation, data integrity and traceability concerns have to be taken into account along with potential threats and attacks. Referring more specifically to many IoT devices, fall back plans and mechanisms to introduce a tamper-proof environment are needed. Finally, the decentralised technology of Blockchain has been indicated as a key enabler for network security and trust. 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.

3.2.2 AUTOPILOT

Industrial Control System:

AUTOPILOT focuses on the application of IoT to the automotive and autonomous vehicles markets and a specific activity is devoted to cope with cybersecurity threats.

In order to quantify the cybersecurity threats, it is important to list the information assets which must be protected and to understand their importance to the various stakeholders.

An "Authentication" process is needed too. It means assuring the authenticity of every sensor that composed the wireless sensors network (WSN) and that is involved in the wireless communication process among vehicles and infrastructures.

To assess security and privacy issues in AUTOPILOT, threats and countermeasures have been defined by referring directly to the main current standards.

Building Blocks:

AUTOPILOT network is mainly built by three building blocks: the in-vehicle connectivity network, the Cloud IoT platform, and the V2X (Vehicle-to-Everything) and IoT network of connected devices.

The in-vehicle IoT network is the most critical zone of the system that requires a specific attention to provide the highest security level, due mainly to some novelty aspects compared to the other two blocks; the IoT & V2X zone covers the medium range communications between the vehicle and its close surroundings whereas the IoT Cloud Platform collects and exploits data from IoT peripheral devices and provides feedback control/navigation/optimization data to peripheral devices.

AUTOPILOT as a GDPR private information processor:

AUTOPILOT solution may be viewed as a private information processor from GDPR (General Data Protection Regulation) point of view. The private information processor enters the system on several levels as the user may be directly registered to the end-user services or may enter the system with their devices. The private information may also be collected collaterally as a part of video data or similar ones from various kind of sensors.

Privacy requirements are an integral part of the AUTOPILOT specification. They were defined

in the initial stage of the project and will be assessed during evaluation of each pilot site; they cover privacy and data flow assessment and risks minimization; GDPR compliancy; strong authentication and authorization and audit log for publicly accessible services and translation of the credentials between layers of the system.

Security:

Security is the ability of the autonomous vehicle system, including IoT technologies, to protect the users/passengers, the pedestrians and other road users, the system itself and the information from unauthorised actions, deliberate and accidental intrusion or attacks [6]. The trust is influenced by the security level of a system and is particularly important in autonomous vehicle applications.

Security measures are implemented in the information system in order to mitigate security risks. Security is one of the main concerns regarding IoT, which needs to be addressed along with the paramount need for safety [7]. Security attributes is one of the main determinants for users to accept the autonomous vehicles, IoT and AI (Artificial Intelligence) applications. Security relates to an attribute that protects the digital information and data from any danger or threat from any malicious.

Information security addresses the protection goals confidentiality, integrity, availability. These goals are important and also form a privacy and data protection perspective that specifically requires that unauthorised access and processing, manipulation, loss, destruction and damage are prevented [8].

Components of the system, the services that they and the system use, and the services the system provide shall be secure [9]:

- By design – the product, or service has been conceived, designed and implemented to ensure the key security properties and maintained: availability, confidentiality, integrity and accountability.
- By default – the product, or service, is supplied with the confirmed capability to support these security properties at installation.
- Throughout their lifecycle – security should be maintained from initial deployment through maintenance to decommissioning.

Security in an autonomous driving IoT systems is more than just information security because assets are not just data and IT infrastructure, and because securing a distributed network of devices presents different challenges.

The IoT policy framework regarding security for autonomous vehicles applications which underlies the recommendations are summarised in Figure 6 [6].

Figure 6: Autonomous vehicles IoT security framework [6]

Good security practices are of fundamental importance [6]. Even if there will probably never exist a finite set of tools and practices that can mechanically protect against all threats, what is

very important is to raise awareness about security among all the stakeholders.

For system developers, maintainers and integrators following risk based secure development is paramount. Awareness at all levels and technology that does not impede usability and does not "get in the way" of user interactions with the systems are the keys to develop security properly. The protection of smart vehicles depends on the protection of all systems involved (cloud services, applications, car components, maintenance and diagnostic tools, etc.) [6][11].

The risk to the driver, their passengers and other users of the road makes it a matter of national end European interest. For this purpose, the following recommendations have been developed [6][11]:

- Recommendations for smart vehicle manufacturers, tiers and aftermarket vendors:
  - Improve cyber security in smart vehicles.
  - Improve information sharing amongst industry actors.
  - Improve exchanges with security researches and third parties.
- Recommendations for smart car manufacturers, tiers, aftermarket vendors and insurance companies:
  - Clarify liability among industry actors.
- Recommendation for industry groups associations:
  - Achieve consensus on technical standards for good practices.
  - Define an independent third-party evaluation scheme.
- Recommendation for industry groups and associations and security companies:
  - Build tools for security analysis.

It is important to understand that software vulnerabilities can have a scope beyond the software itself. Depending on the nature of the software, the vulnerability and the supporting infrastructure, the impact of a successful exploitation can include also the software and its associated information, the operating systems of associated servers, the backend database other applications in a shared environment, the user's system, and other software that the user interacts with [6][12].

Table 1 provides a list of security related requirements and recommendations identified by the AUTOPILOT partners, applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA (Online Trust Alliance) [6][13], and ENISA (European Union Agency for Cybersecurity) in "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [6][7].

Table 1: Security - Requirements (Req) and Recommendations (Rec) [6]

Security framework	Req.	Rec.
Raise awareness for the need for IoT cybersecurity in autonomous vehicles and IoT systems, promote harmonization of cybersecurity initiatives and regulations, and foster economic and administrative incentives for cybersecurity.	X	
Achieve consensus for interoperability across the autonomous vehicles and IoT ecosystem and clarify liability among the stakeholders.	X	
Ensure and substantiate the robustness against all types of attack vectors in the IoT systems based on AI mechanisms. This includes securing each AI mechanism system itself, as well as securing the communication between edge computing devices or vehicles with for example encryption and authentication mechanisms against attacks.	X	
Disclose whether the autonomous vehicles IoT system is able to receive security related updates. If yes, disclose if the systems' constituent parts can receive and update security updates automatically. If any user action required, explain what user action is required to ensure correct update.	X	
Disclose what and how autonomous vehicles and driving features will fail to function if connectivity or backend services becomes disabled or stopped, including potential impact and necessary action. Include also the potential consequences and necessary action if the system/device no longer receives security updates.	X	

Ensure mechanisms is for automated safe and secure methods to provide software and firmware updates, patches and revisions. Such updates must be verified as coming from a trusted source.	X	
Ensure IoT devices, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, cellular (e.g., 4G) and Bluetooth connections.	X	
All IoT support web sites must fully encrypt the user session, from the device, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, to the backend services. Current best practices include HTTPS and/or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, should include mechanisms to reliably authenticate their backend services and supporting applications.	X	
Ensure all IoT devices, including autonomous vehicle including its embedded IoT gateways, sensors and actuators, and associated software, have been subjected to a rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modelling, along with maintaining an inventory of the source for any third party/open source code and/or components. Employ generally accepted code and system hardening techniques across a range of typical use case scenarios, including preventing any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. IoT devices should ship with current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	X	
Define secure software and hardware development lifecycle guidelines for autonomous vehicles and IoT; and establish secure autonomous vehicle and IoT products and services lifecycle management.	X	
Design IoT devices, such as autonomous vehicle including its embedded IoT gateways, sensors, and actuators, to minimum requirements necessary for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.	X	
Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain use cases a user may want the ability of deciding how and when the updates are made including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely automatic updates are pushed to the IoT device seamlessly without user interaction and may or may not provide user notice. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors and actuators.	X	
Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	X	
Implement measures to help prevent and make evident any physical tampering of autonomous vehicle system and its constituent parts (e.g. IoT devices). Such measures help to protect the system and its AD functionality from being modified for malicious purposes.	X	
Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to vehicle and product features, functionality, security, and privacy.	X	
Disclose the duration and end-of-life security and patch support, (beyond product warranty). Ideally such disclosures should be aligned to the expected lifespan of the device. It is recognized IoT devices cannot be indefinitely secure and patchable. Communicate the risks of using a device beyond its usability date, and impact and risk to others if warnings are ignored or the device is not retired.	X	

If the users must pay any fees or subscribe to an annual support agreement this should be communicated/disclosed prior to the purchase, and security related functions or other important functionalities should not stop working due to non-payment.	X	

Privacy:

The notion of privacy refers to all the organisational and technical measures implemented for any processing of personal data in order to guarantee the protection of such data and the rights of the data subjects [6]. Privacy refers to the data used by the autonomous vehicle system, including IoT technologies. More precisely, it refers to how these data are used and by whom.

For autonomous vehicles, IoT and AI applications the privacy must be considered from different angles in order to address the complexity of different issues [6]. Privacy in the case of autonomous vehicles, IoT and AI applications should be considered to be contextual, in the sense that information flows of personal information could be seen as appropriate or not depending on the context where these flows happen, and each context could have a number of norms, or rules that govern the flow of personal information. Privacy in human to human relationships is focusing on how individuals interact with others, continuously negotiating the information they reveal/conceal to/from others.

In autonomous vehicles, IoT and AI applications there is a need to acknowledge the plurality of privacy, focusing on the information-related activities, how the activities are performed, what type of data is involved, who uses/handles/transfers/stores the data, personal and cultural factors, habits, preferences, etc. [6].

Detecting when and where a privacy breach may happen when dealing with personal information and hence privacy-respecting mechanisms in autonomous vehicles, IoT and AI applications and what specific mechanisms and how they could be used to design privacy-respecting autonomous systems need to be addressed.

The trust is influenced by the privacy information generated and used by a system and is particularly important in autonomous vehicle applications.

The IoT policy framework regarding privacy for autonomous vehicles applications which underlies the recommendations are summarised in Figure 7 [6].

Figure 7: Autonomous vehicles IoT privacy framework [6]

Table 2 provides a list of privacy related requirements and recommendations identified by AUTOPILOT partners, applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA [6][13].

Table 2: Privacy - Requirements (Req) and Recommendations (Rec) [6]

Privacy framework	Req.	Rec.
Provide and disclosure data solutions for the autonomous vehicles and IoT ecosystem in accordance with GDPR.	X	

If IoT systems based on AI mechanisms operate on mission critical data which shall remain private, process such data locally at the edge and only leverage data available within privacy limits.		X
Provide accurate and understandable disclosures of all the relevant autonomous vehicles service providers' privacy practices in accordance with applicable laws and regulations.	X	
Ensure that privacy together with security and support policies are accurate and understandable, and easily available for review prior to purchase, activation, download, or enrolment. In addition to prominent integration and placement suitable for the autonomous vehicle applications, the information should be available on product packages, websites, and contracts.	X	
Updates and patches must not change privacy settings or modify user configurated privacy preferences without user notification. If changed or modified, the user must be provided the ability to review and select privacy settings on the first use.	X	
Aim at data minimisation; only necessary data for the autonomous vehicle applications should be collected, transmitted, stored, shared and used.		X
Ensure and disclosure the rights of the data subjects and the right to data portability.	X	
Disclose the data storage policy and storage duration of personally identifiable information.	X	
Explain clearly what personally identifiable and sensitive data types and attributes are collected, how they are used, and how privacy is ensured. Limit the collection to data which are necessary and useful for the autonomous vehicles' application functionality and purpose. If the collected data are used for other purposes than intended, the consumers and other relevant stakeholders must be informed and obtain acceptance.	X	
The system can limit data access according to the "need to know" principle. The system can separate the sensitive data and apply specific access control policies. The system can also encrypt sensitive data to protect their confidentiality during transmission and storage. Access to temporary shadow files which are produced during the data processing must also be protected.	X	
Encrypted data communication would reduce the potential privacy risks due to unauthorised access during data transfer between components. There are multiple data communication approaches based on the components involved in an IoT application, namely, 1) device-to-device, 2) device-to-gateway, 3) device-to-cloud, and 4) gateway to-cloud.		X
Provide guidance on best practices in notification in privacy policies and also require to companies to collect feedback to assess consumers' comprehension of privacy policies. Manufacturers disclose what sensors are onboard devices and what they collect, in order to expand the definition of personally identifiable information to include data collected by IoT sensors.	X	
The IoT ecosystem has multiple stakeholders who play significant roles in providing end-to-end IoT service. The privacy warp should run through the fabric of IoT components as a key enabler for all stakeholders to provide full functionality along with other key requirements like security and safety.		X
The vendor must allow users to access their collected data, free of charge, submitting a link to its public privacy policy explaining how the collected data is used. The vendor must allow users to migrate their collected data to another backend and to delete their collected data, with public documentation explaining how to restrict and/or update the use of the collected data The vendor must allow users to easily opt out of direct marketing based on their collected data.	X	
The vendor must make explicit the expected duration of the terms of service, the legal implications of substantially changing device usage and must ask permission from users before changing the terms of service or for upgrade firmware.	X	
The vendor should grant third party clients the same functional scope on the backend as its own clients and allows third parties to connect clients/devices to its backend (also direct communication with its devices, without going through the backend).		X

Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors, and actuators.	X	
IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors, and actuators.	X	
Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	X	
Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to privacy.	X	

Trust:

Trustworthiness is a property of people that engenders trust in the autonomous vehicles system, including IoT technologies [6]. 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. There are several criteria that influence the trust that users can have on autonomous vehicle system and IoT technologies. For example, they need to be sure that the system is not increasing the risks on roads or to know how their data are used. The clients' truth is one of the main points of autonomous vehicles and IoT policy framework, it is necessary to work on the reputation of the system and on the transparency with the user.

Important for the notion of trustworthiness is reliability and accuracy as autonomous vehicles, IoT and AI systems are trustworthy if the users and other autonomous systems can rely on them being right [6]. Reliability is necessary for trust in autonomous vehicles, IoT and AI systems but is not enough. In this context, there should be considered the difference between human-human trust and human-AI-autonomous trust violations as there are different levels of competence required for humans to trust other humans versus trusting AI.

Trust built up inductively between humans and autonomous systems IoT and AI can be destroyed with single instances of inaccuracy or unreliability. Building trustworthy autonomous vehicles, IoT and AI systems requires understanding trust in human-human relationships, human-autonomous systems and autonomous systems to systems interactions.

The IoT policy framework regarding trust for autonomous vehicles applications which underlies the recommendations are summarised in Figure 8 [6].

Figure 8: Autonomous vehicles IoT trust framework [6]

Table 3 provides a list of trust related requirements and recommendations applicable to IoT enabled autonomous driving environments. Note that some of the points are based on

requirements and recommendations given by OTA [6][13].

Table 3: Trust - Requirements (Req) and Recommendations (Rec) [6]

Trust framework	Req.	Rec.
Ensure and substantiate the accuracy and quality of the data that are used by the AI learning algorithms which influences the decisions of an IoT application involving autonomous vehicles. In these safety and mission critical applications reliable data are crucial. The use and processing of data from reliable sources are an important element in maintaining confidence and trust in the AI technology and its mechanisms.	X	
Achieve trust and trustworthiness by ensuring and proving excellent safety, security, privacy, resilience, reliability, and dependability properties for the autonomous vehicles and driving applications.	X	
Achieve trust and trustworthiness by ensuring high quality of information, service and experience (QoI, QoS and QoE) for the autonomous vehicles and driving applications.		X
Updates and patches should not modify user configurated settings without user notification. If modified, the user should be provided the ability to review on the first use, and if not safety/security/privacy critical the ability to select settings.	X	
Validate that the system gets the waited data in requested time (latency requirements for that function), otherwise the data will be outdated.	X	
Do not hand out users' information and data without the users' permission	X	
If you need to transfer users' information or data to another third part, you should share only the needed users' information and data.		X
Verify that your system gets the needed data at every moment even in the worst-case situation.		X

IoT Security, Privacy and Trust:

The recommendation for designing security and privacy are provided by the AUTOPILOT project in deliverable D5.4 under two items: "Autonomous vehicles IoT security framework" and "Autonomous vehicles IoT privacy framework" [6][10]. 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.).

AUTOPILOT has provided several recommendations for assuring security and privacy in delivery D5.4 [6]. 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 Design and Cyber Security and Resilience of smart cars), OWASP (Open Web Application Security Project), NIST (U.S. National Institute of Standards and Technology) Cybersecurity Framework and emerging needs based on the specific issues brought by autonomous vehicles and IoT technologies.

The social and economic implications of autonomous vehicle technologies affect all the stakeholders in the new created autonomous vehicles and IoT ecosystem [10]. 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 its information secure and private for the required cases is a critical element for the public trust, 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, and security to assure working towards 99,999999%reliable systems (e.g., increased reliability, built-in fail operational mechanisms, minimise the threat of cyber-security attacks and SW/HW bugs etc.) 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).

The autonomous vehicles are expected to bring significant benefits in terms of fuel efficiency, reduced emissions, saving time and safer mobility [10]. 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 and disruptive 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.

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 [10]. 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.

3.2.3 IoF2020

Use Cases Interviews

During the project kick-off meeting all 19 (heterogenous) use case owners were interviewed by asking them a couple of questions regarding their approach towards securing the use case at stake. By doing so the researchers got a first glance at a situation which was and largely still is characterized by a lack of awareness, understanding and also available solutions to guarantee a robust level of security and privacy throughout all use cases.

Security Analysis Exercise

Throughout the first year of the project, NXP prepared a STRIDE security analysis exercise, which each use case carried out. This substantial and in-depth analysis of the results enabled to

identify the risks and weaknesses of each use case when it comes to security. The researchers have analysed the results and prepared a first overview of technologies and mechanisms that can help use case owners to increase the security and privacy levels within the use cases. The goal is to help and monitor the implementation of the proposed measures and then conduct a second STRIDE analysis to clearly depict the progress made.

Standard Data Sharing Agreement

Researchers have not identified specific categories of personal data of interest for the project. They have produced a standard data sharing agreement for service providers and their test farms to secure the data usage.

Other Enablers

IoF2020 has developed a set of enablers to support full data protection, including:

- Data Dashboard for farmers to control and monitor the exchange of their data.
- Transparent on-boarding process for farmers to gain trust in technology.
- Risk-analysis based on CNIL (Commission Nationale Informatique & Libertés) guidelines and ISO/IEC 27552.
- Creation of a new Work Package (WP6) on ethics and privacy that coordinated activities in the field.

IoT Security, Privacy and Trust:

Through the scope of WP3, the 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 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. Farm management information systems (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.

Through the IoF2020 project, 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. Through WP7 it has developed an overview over ethical issues that are encountered in the use cases and which also include issues about privacy. IoF2020 procedures are developed to discuss such arrangements between participants of the use cases. Insightful gap analysis feedback addressing this topic are carried out in WP3.

A cyber-security analysis was carried out on several use cases using the STRIDE methodology and has been useful to make sure that design and specification activities also accounted for security aspects. The STRIDE analysis is most effective when applied to complete, operational

systems, also considering organizational and business-related aspects.

Regarding security-related aspects, it is difficult to plan technical and architectural aspects when the data ownership and 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 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.).

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 must 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. 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. 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.

3.2.4 MONICA

Privacy strategy-Security assessment

Researchers have had regular meetings to discuss security and privacy issues with the partners of the project. Furthermore, the project partners have conducted an assessment to work closely together to ensure that security is considered in the product design.

Risk Analysis

MONICA has performed a risk analysis. The approach taken with the security assessment has been to consider threat scenarios and to consider how provisions can be put into place to protect against potential attacks (e.g. replay and masquerade, DoS attacks).

GDPR compliance

On the privacy side, the GDPR has been considered as a priority by MONICA. MONICA researchers have considered not only GDPR but also other EU standards, such as the NIS Directive. MONICA also leveraged on the interaction between the different LSPs projects, which has been very helpful when considering data protection requirements.

IoT Security, Privacy and Trust:

The MONICA project leverages the collective awareness platform for sustainability and social innovation (CAPS) which is the crux for trust in a smart city. The CAPS complement existing initiatives that support citizen involvement in the utilisation of open data. MONICA has integrated (Copenhagen and Torino) data from various open data platforms into the CAPS and enable access to new open data coming from the project. This allow for improved efficiency of public services, and economic growth to social welfare. 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.

The main concerns regarding trust is that 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.

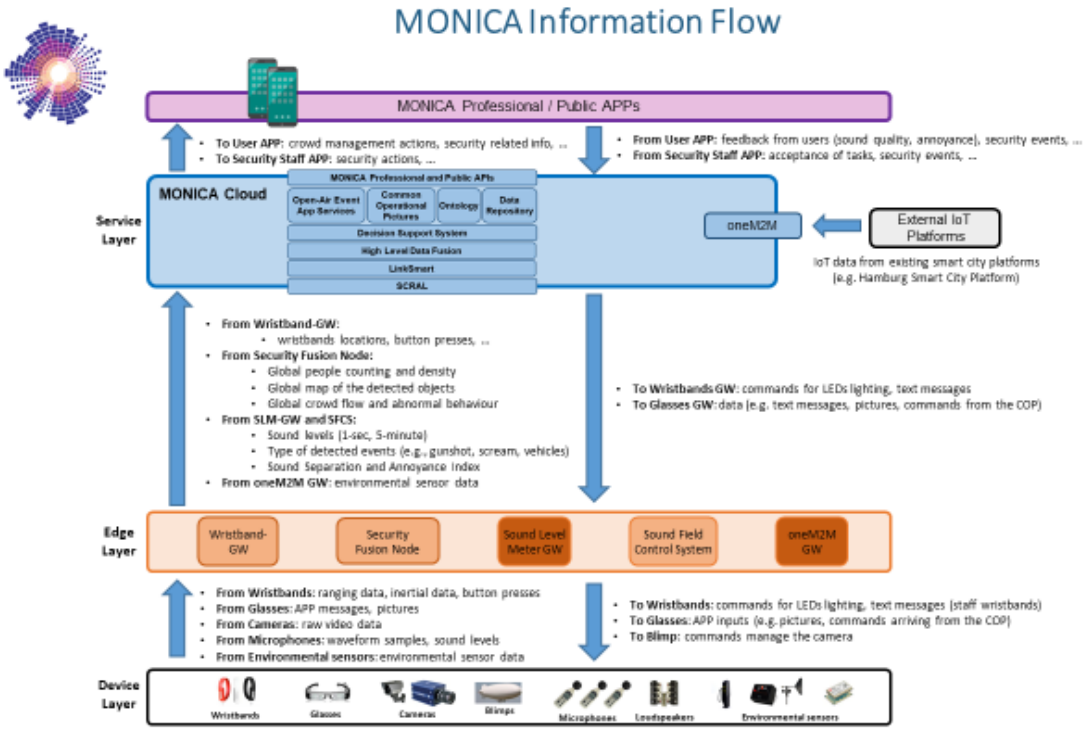

Figure 9: MONICA Information flow

During the MONICA project an ethical assessment on how data from pilots is managed within the project was conducted. Moreover, Data Protection Impact Assessments (DPIA) have been performed for each pilot. The results of the assessment show that pilots are in compliance with the project's Ethical Guidelines and the applicable regulatory requirements, notably the General Data Protection Regulation (GDPR).

Compliance with the project's Ethical Guidelines

This assessment is based on the project's Ethical Checklist; a tool to help partners assess if there are any ethical issues or concerns in relation to the pilot demonstration. The Ethical Checklist places the data subjects in the centre, focusing on assessing if there are any ethical problems with how their personal data is collected, processed and shared in the MONICA project. The Ethical Checklists have been completed for personal data only and the checklist itself was useful

in determining which data (potentially) constituted personal data.

Data Protection Impact Assessments (DPIA)

DPIA have been conducted for the use cases collecting and processing personal data as well as for the Common Operational Picture (COP) and the Live Positioning System (LiPS). DPIAs have been performed for all the relevant use cases demonstrated in the pilots.

Technical partners have been consulted with respect to the Data Flow for the different solutions and with respect to the DPIAs. The figure below illustrates the overall data flow in MONICA.

The DPIAs have been approved by the pilot owner and the project's Ethical Manager. Figure 9 illustrates the overall data flow in MONICA.

Data Management Plans (DMP)

Data Management Plans (DMP) were created for each use case the individual pilots demonstrated. The DMPs were created following the general guidelines defined in MONICA project. The DMPs were consulted in connection with the completion of the Ethical Checklists and DPIAs

3.2.5 SYNCHRONICITY

SYNCHRONICITY

Data Protection Impact Assessment Tool for Smart Cities

A Data Protection Impact Assessment (DPIA) tool for smart cities has been developed by MI to address the specific needs, requirements, and risks related to IoT deployments in smart cities. This DPIA has been applied by all the participating cities to Synchronicity. It is used to enable the Data Protection Committee of the project to overview the compliance of each participating city with the GDPR. The DPIA is intended for all cities participating in Synchronicity, as well as for any other interested smart cities.

Privacy App

Privacy App is a freely available smart phone application developed by MI. It enables smart cities to inform their citizens on the IoT solutions deployed on their territory. It provides information on the purpose for data collection, who is the data controller, the data retention period, who can access the data, etc. It is a collaborative tool: it enables citizens to report any newly identified IoT device in the city, as well as to directly contact the data protection officer of any deployed IoT device. It is freely available for Android and iPhone smart phones. Privacy App is intended for all cities participating in Synchronicity, as well as for any other interested smart cities, and will be promoted through the Open and Agile Smart Cities Alliance (OASC).

GDPR Certification

The City of Carouge is using EuroPrivacy certification scheme to systematically assess its compliance with the GDPR obligations. EuroPrivacy has been developed in the H2020 research project Privacy Flag to enable a more systematic assessment of the compliance with the GDPR. It covers emerging technologies, such as IoT and smart cities domain. The EuroPrivacy certification scheme is managed by the European Center for Certification and Privacy (ECCP) in Luxembourg with the support of an international board of experts in data protection. It has been submitted by the authority of Luxembourg to the European Data Protection Board as an official certification scheme according to article 42 of the GDPR.

IoT Security, Privacy and Trust:

Through the SYNCHRONICITY project, high level concerns on security and privacy have been identified like: Generic statements relating to the importance of citizens privacy; statements that relate to transparency of the underlying processes and polices in how cities handle IoT

generated data; statements that restrict what IoT data should be collected from an IoT infrastructure in a city; statements that refer to the compliance of IoT data handling with respect to laws and regulations; statements that refer to anonymization of personal identifiable data and its potential caveats; and statements that outline conditions on how collected IoT data should be shared.

It is important to consider the different logical components of the 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 through: Context Data management; IoT Management; Data Storage Management; IoT Data Marketplace; Security, Privacy and Governance; and Monitoring and Platform management services.

SYNCHRONICITY is a smart-city project and 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.

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 properties like: 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; and Common legal foundation. Overcoming the barriers identified requires a common approach across the different cities.
This approach needs to consider of the following elements:

- 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.
- 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.
- 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.
- 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.

3.3 U4IoT CSA contribution

U4IoT project is a coordination and support action (CSA) and supported the activities with the following tasks.

Serious Game on Data Protection for LSPs

A serious game on data protection has been developed by AS to raise awareness and train LSPs in respecting the GDPR obligations. The privacy game is made of cards with questions enabling players to assess and increase their level of understanding of the GDPR principles and obligations. An extension of the game towards an online game is in process, as well as another version tailored for SMEs (Small and Medium-sized Enterprises). The game is intended for all LSPs, as well as for SMEs and the public at large.

Guidelines on Personal Data Protection for LSPs

A set of practical guidelines have been specified by AS to support the implementation of the GDPR obligations by the LSPs. It provides an overview of the main GDPR obligations, their implications for LSPs, as well as practical processes and checklists to ensure a full compliance of the LSPs with these obligations. The guidelines are intended for all LSPs, as well as for other interested H2020 research projects.

4. THE COMMON EVENT

The chapter describe the format of the event and summarise the discussions among the representatives of different projects that refer to their different privacy and security approaches and to the different enablers which they have developed.

4.1 IoT security and privacy addressed by the LSPs

Data protection and security are to be understood as closely interconnected even though they are separate concepts as "while security techniques are indeed relevant to support data protection and privacy, they do not guarantee per se the principles of privacy" [1] and therefore "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 a different degree of conflict" [1].The framework proposed by CREATE-IoT is based on a principled-based approach which considers the principles and measures identified by the GDPR (arts. 5-11 and 32) and also ISO standard 29100 a more general principles like: purpose limitation, data minimization, proportionality, transparency and accountability. The principles need to be made operation by implementing them through a privacy and security by design engineering methodology. The interaction of these principles and basic concepts in the context of the IoT policy framework was discussed in the event also taking into consideration recent policy developments.

4.1.1 The Common event

The first day of the workshop was of relevance for the topics of data protection and security as it was centred around the presentation of the results of the ETSI Specialist Task Force (STF) 547. The main guidelines for privacy and security in IoT were presented:

Table 4: ETSI STF Technical Reports

No	Title
TR 103 591	Privacy Study Report – Standards Landscape and best practices
TR 103 533	Security Study Report – Standards Landscape and best practices
TR 103 534-1	Teaching Material – Part 1: IoT Security and Teaching material
TR 103 534-2	Teaching Material – Part 2: IoT Privacy and Teaching material
TR 103 535	Guidelines for using semantic interoperability in the industry
TR 103 536	Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms
TR 103 537	Plugtests preparation on Semantic Interoperability
SR 003 680	Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach

During the discussions, the focus has been on the role of standards in support of data protection and privacy regulation and security. Many participants agreed on the need to be more proactive in the different SDOs (Standard Development Organizations) in the support of standardization initiatives in the field where European driven initiatives seems to be lacking. Security methodologies were also discussed, security by design, and the need to adapt the different methodologies to the different application domains.

Also, the question of the definition of security was tackled especially taking into consideration the peculiarities of an IoT ecosystem. Typical characteristics discussions have been:

- The role of the different stakeholders.
- The role of data protection.
- The interoperability requirements.

- Security as an enabler for trust and safety.
- The needs to integrate different technologies in an IoT ecosystem.
- The relationships between IoT, Cloud, and Edge Computing.
- The role of legacy in IoT ecosystems.

The increasing importance of certification schemes for IoT was also discussed. As we treated in deliverable D05.05, the initial Legal IoT Framework [14], and summarized in our deliverable D06.11 report: "IoT security is difficult yet essential, with attackers having greater access to the toolkit for exploiting IoT compared to many other ICT systems. Risk, liability, and responsibility is shared across a much greater set of actors. IoT is a catch all term covering many complex elements, e.g. virtual networking, mobility, cloud services, composite services and distributed services" [4]. The presentations and discussions on data protection focused on the definition of the concept of privacy, the categories of different personal data and the role and rights in the context of the GDPR, understandings and definitions of privacy and security. A detailed survey of the discussions has been reported in deliverable D06.11 [4].

As mentioned, the five LSPs and the two CSAs have worked to capture the lessons learned in the different research projects to extract the recommendations and good practices stemming from the different researches. This has led to different discussions in the context of AG05. It was decided not to use the term '*White Paper'* as it is usually associated with Commission's documents. The most interesting part would probably be chapter seven where it is possible to find guidelines and recommendations. There is the willingness to work on a declaration to be approved ad the IoT Week based on the work done to draft the guidelines. The document will also be updated for a new release of the guidelines in order to consider the feedback from the new projects.

The session on IoT Security, privacy policy framework was moderated by Peter Wintlev-Jensen and Salvatore Scalzo (EC) and offered the opportunity to reflect on key issues which can be summarized as follows:

- The LSPs have all add security and privacy dimensions. All involved privacy and security risk analysis. There is no need to use the same methodology as far as the risk analysis is done. One thing that needs still to be considered is that privacy and security go hand in hand, and you cannot really separate them. If you take the state of the art, the LSPs cannot go until the end especially as far as assurance and certification are concerned. This is one of the challenges for the future, especially considering the change in the regulatory landscape. These are the steps that guarantee trustworthiness of the ecosystem.
- It was argued that we are still mixing privacy and data protection. But the GDPR uses the term 'privacy' only in footnotes. It was considered that the focus should be data protection. We still need to clarify this. It is not only semantic. There is a need to bring together the different actors of the value chain to work on real data protection by design and not only security. IoT, AI and data analytics is another topic of extreme importance.
- Interaction between data protection, privacy and ethics. All these notions should come together and interact.
- It was argued that addressing liability issues also will be key, we have clearly seen this in the context of smart cities. It was asked, who is responsible for the handling of data in this ecosystem? Definition of controller and co-controller need to be considered.
- There is the need to facilitate the circulation of the lessons learned in the pilots to facilitate future projects.
- It was emphasised that it is important to assess what happens after the review of the projects and to facilitate the transition to the market of the different solutions. Probably we should be able to identify which solutions could be supported for a full transition to the market. This helps in preserving value creation from research projects.
- Model of the ERC-proof of concept. This model can be replicated for projects transition to market.

- The projects have incentivized certain stakeholders to learn about data protection and implement appropriate solutions. A data protection by design strategy for each project could probably be foreseen to give Europe a competitive advantage on the global market. This increase in trust can make a global difference for European products.
- It is important that each project develops its own privacy plan also within each pilot. This should be done at the design level, at architectural level. Workshops with pilots should be organized at the local level to implement and check the design. This would also facilitate to solve the issue of liability within projects.
- It was argued that we always have issues between interoperability and security. Need to develop risk assessment for the key use cases. Thanks to the architecture we have developed a structure to address security issues. Projects facilitate complementarity in this context.
- Risk analysis and compliance should be separated as they are two different things. It would be interesting to have a peer-review process for assessing compliance and risk analysis for the projects. Maybe we can also support dedicated actions to support compliance and risk analysis.
- Avoid the risk of fragmentation in standards as different legal requirements are being developed in different parts of the world. This is important in certification both for cybersecurity and data protection.
- Data ownership needs to be further discussed also for what concerns liability; the same goes for the metrics on data quality.
- It is not enough to work on standardization only at the European level as by doing so you lose important market opportunities. Therefore, it is important to work at the global level with global SDOs.
- One thing worth noticing is that it might seem a paradox, but there are several important companies that work on GDPR compliance and they are American companies. We should investigate more why Europeans are not able to produce global companies.

4.1.2 The LSPs Pilots workshop

The second day of the workshop focused on the handover of common activities from the IoT LSPs cluster to the DEI LSPs cluster. The different projects had the possibility to refer to their different privacy and security approaches and to the different enablers which they have developed. In the Stream 4 session on Innovation support deliverables such as the document on "*Personal Data Protection for Internet of Things Deployments: Lessons Learned from the European Large-Scale Pilots of Internet of Things*", the IERC Cluster Books, the Security approach, the KPIs (Key Performance Indicators) for the LSPs, the eBook, the IoT Handbook.

4.2 The New Data Strategy

During the event, on February 19th, 2020, the EC announced its new Digital Strategy highlighting that digital transformation, trust and AI are one of the priorities for the EU.

The Digital Strategy is an important development for the research and business community, and it is based on three pillars:

- Open access to data.
- Creation of an infrastructure to run processes that act on data.
- Specific sectorial actions on creating data spaces

The Digital Strategy proposed by the Commission will have an important impact for the IoT ecosystem. In the Digital Strategy the Commission proposes an approach based on four pillars:

- A cross-sectoral governance framework for data access and use that will cover, among other measures, new EU mechanisms and guidance on data sharing.
- Investment in data and EU capabilities and infrastructures for hosting, processing and using data.

- Investments in digital skills and in SMEs.
- Development of European common data spaces in strategic sectors and domains of public interest

The White Paper on Artificial Intelligence [22] aims at developing the EU capabilities in the field. The development of AI is of relevance for the IoT ecosystems given its potential as an enabler. The Commission aims at taking several steps:

- Review and update its 2018 Coordinated Action Plan on AI.
- Facilitate the creation of AI excellence and testing centres.
- Promotion and development of AI by the public sector.
- Promotion of a public-private partnership in AI, data and robotics.
- Investments in educating and upskilling the workforce on AI skills.

The Commission also addresses the need to develop an ecosystem of trust. An element of the ecosystem will be constituted by proposals for a regulatory framework for AI and the introduction of mandatory pre-marketing conformity assessment requirements to be applied to high-risk" AI applications. In depth discussions relevant for the IoT ecosystem can also be found in the Commission's report on the safety and liability implications of AI, IoT and robotics accompanying the White Paper [22].

5. CONCLUSIONS

5.1 Key takeaways

The event has offered the opportunity to discuss the role of the of privacy and security in the context of the IoT Policy Framework. The takeaways and findings are summarised as following:

- Data protection and security are to be understood as critical building blocks of the IoT ecosystem. They must be designed embedded in the devices by applying the best privacy and security design methodologies.
- The strategy in the context of the ecosystem will have to contemplate the different ranges of risks and purposes of the various markets, sectors, and domains.
- The IoT policy framework must focus on consumer and industry trust through hardened data protection.

The findings that are relevant for the IoT stakeholders and the partners of the LSPs consider the role of the framework in the context of the project activities:

- LSPs have addressed the issues concerning privacy and security overall successfully.
- Risk management principles and security/privacy by design have generally applied.
- Requirements/checklists were produced.
- Lack of assurance path is seen as a major problem.
- The use of the terms “data protection” and “privacy” needs to be clarified.
- There has been a strong multi-stakeholder engagement in the context of the LSPs.
- A need for multidisciplinary approaches in analysing these issues has been detected.
- Ethics is seen as a separate and crucial dimension.
- There is a positive consideration of data protection as one of the objectives of the LSPs.
- Future assurance/certification schemes are highly beneficial.
- Multidisciplinary/multi-stakeholder approach in addressing these issues is essential.
- Setting of legal responsibilities for actors other than manufacturers to be considered.
- Need for strong interaction between data protection and ethics.
- Need for model/mechanism to screen and identity project outputs that could be really exploited and moved forward when the project ends.
- Projects have to be invited to introduce requirements for data protection strategy (together with exploitation plan).
- Links among different projects need to be strengthened, notably on privacy/security issues (make the best possible use of relevant cluster), including sharing templates.
- Education aspect is seen as important (both on demand/supply side).
- Need for standardisation in the field (with two caveats: 1. Global level standardisation; 2. Standardisation is unlikely to cover all aspects).
- Considering tools to map standards vs legal requirements.
- Cross-fertilization among project practices is seen as essential.
- Develop practices/methodologies to deal with lifecycle related aspects.
- Adapt regulation/standardisation to the ecosystem concept.
- Specific issues linked to algorithms (e.g. anonymisation)

5.2 Follow-up

The CREATE-IoT IoT policy framework and the best practices from the LSPs can be used as reference elements during the discussion on the EC new policy cycle. The new Data Strategy, the development of the AI framework, the regulation on security and liability will all impact the

development of the IoT policy framework and vice versa. These dimensions will all need to be investigated in the new projects and coordination activities.

The CREATE-IoT IoT policy framework forms the basis for the coordination of next wave of LSP projects and the lessons learned are offered in hindsight for making collaboration between the projects more fruitful.

6. REFERENCES

[1] IoT European Large-Scale Pilots Programme portal. Online at: https://european-iot-pilots.eu/

[2] CREATE-IoT project. Online at: https://european-iot-pilots.eu/create-iot/

[3] CREATE-IoT, Deliverable 05.01 - *IoT Policy Framework*, October 2017. Online at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf

[4] CREATE-IoT, Deliverable 06.11 - *Workshop on common IoT standardisation framework*, March 2020.

[5] S. Ziegler et al., Personal Data Protection for Internet of Things Deployments: Lessons Learned from the European Large-Scale Pilots of Internet of Things, v. 8.5, February 2020.

[6] AUTOPILOT, IoT Policy Framework for autonomous vehicles applications (D5.4). December 2018. Online at: https://autopilot-project.eu/deliverables/

[7] Privacy and Data Protection by Design (from policy to engineering). ENISA, December 2014

[8] Indispensable baseline security requirements for the procurement of secure ICT products and services, v.1.0 (Public). ENISA, December 2016

[9] OWASP Secure Coding Practices, Quick Reference Guide, v.2.0. The OWASP Foundation November 2010, online at: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[10] CREATE-IoT, Deliverable 05.02 - IoT Policy Framework Evaluation and Final IoT Policy Framework, January 2020.

[11] Cyber Security and Resilience of smart cars. ENISA, December 2016.

[12] OWASP Secure Coding Practices, Quick Reference Guide, v.2.0. The OWASP Foundation November 2010, online at: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[13] The Online Trust Alliance (OTA). Internet of Things. Online at: https://otalliance.org/IoT

[14] CREATE-IoT, Deliverable 05.05 - Legal IoT Framework (Initial), December 2017. Online at: https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

[15] ACTIVAGE project. Online at: http://www.activageproject.eu/

[16] AUTOPILOT project. Online at: https://autopilot-project.eu/

[17] IoF2020 project. Online at: https://www.iof2020.eu/

[18] MONICA project. Online at: https://www.monica-project.eu/

[19] SYNCHRONICITY project. Online at: https://synchronicity-iot.eu/

[20] U4IoT project. Online at: https://u4iot.eu/

[21] EuroPrivacy Certification. Online at: https://www.europrivacy.org/en

[22] EC White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, February, 2020 Online at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf