Grant Agreement N°: 101020259
Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D2.2: Use case specification

Work package	WP2
Task	Task 2.1
Due date	31/12/2021
Submission date	30/12/2021
Deliverable lead	Truphone
Version	2.0

Abstract

This public report constitutes the deliverable D2.2 of ARCADIAN-IoT, a Horizon2020 project with the **grant agreement number 101020259**, under the topic **SU-DS02-2020**. D2.2 has the purpose of describing the study around the use cases specification and planning, as well as the legal, ethical, regulatory and social dimensions that relate with the real application cases proposed to validate the ARCADIAN-IoT framework. This study, performed under the task 2.1, will feed task 2.2 with material that allow to specify the requirements that the different components of the framework have. Task 2.1 research also informs task 2.3 with, e.g., knowledge of components articulation and, jointly with the other tasks of WP2, provide context to the research done in WP3 and WP4. Finally, another outcome from task 2.1 depicted in this deliverable is a high-level plan for the use cases implementation towards the project objectives demonstration and validation in WP5.

Keywords: ARCADIAN-IoT use cases; IoT domains/solutions specification; project validation; legal, ethical, regulatory and social dimensions

Document Revision History

Version	Date	Description of change	List of contributors
V1.0	10/12/2021	- First complete version of the deliverable, based on D2.1 content and on partners IPR interests	TRU (editor), All
V2.0	30/12/2021	- Refinement with internal review feedback (submitted version)	TRU (editor), IPN and a SAB member (reviewers)

Disclaimer

The information, documentation and figures available in this deliverable, is written by the ARCADIAN-IoT (Autonomous Trust, Security and Privacy Management Framework for IoT) – project consortium under EC grant agreement 101020259 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Project co-funded by the European Commission under SU-DS02-2020		
Nature of the deliverable:	R*	
Dissemination Level		
PU	Public, fully open, e.g., web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ARCADIAN-IoT project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

This public document represents the deliverable D2.2 from ARCADIAN-IoT project. Its main goal is to report the specification and planning of ARCADIAN-IoT use cases, done in the context of task 2.1. This content is the basis for the specification of the technical requirements of each component of the framework, targeted in task 2.2, which feeds the beginning of WP3 and WP4. Furthermore, this work forms the basis for WP5 regarding the use cases implementation and validation, creating means for assessing the project goals. The research methodology applied in task 2.1 was of iterative nature, aiming for cyclically improving the use cases' specification. Each iteration includes processes of verification and assessment of the use cases' set coherence, relevance and completeness according to ARCADIAN-IoT's goals. The main result of this deliverable is a set of 20 use cases specified and planned considering the perspective of domain experts / solution providers, diverse technology experts and end-users / stakeholders of 3 different IoT domains of application. Considering the agile research approach of the project, the use cases specified in this deliverable will be iteratively assessed and potentially improved after the end of task 2.1, according to the research done in WP3, WP4 and WP5.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AI	Artificial Intelligence
API	Application Interface
CERT	Computer Emergency Response Team
CTI	Cyber Threat Intelligence
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DGA	Drone Guardian Angel
DID	Decentralized Identifier
EDPB	European Data Protection Board
eIDAS	Electronic Identification and Trust Services
eSIM	Embedded Subscriber Identity Module
EU	European Union
eUICC	Embedded Universal Integrated Circuit Card
GDPR	General Data Protection Regulation
GMS	Grid Monitoring Services
ICCID	Integrated Circuit Card Identifier
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
I/O	Input / Output
KPI	Key Performance Indicator
MIoT	Medical Internet of Things
PSK	Pre-shared Key
RoT	Root of Trust
SME	Small and Medium-sized Enterprises
SAB	Security Advisory Board
SoA	State of the Art
SSI	Self-sovereign Identity
UX	User Experience
VC	Verifiable Credentials
WP	Work Package

1. INTRODUCTION

Internet of Things (IoT) technologies, devices and solutions have been penetrating in a wide spectrum of the society day-to-day activities. Recent projections estimate 75.44 billions of connected devices by 2025, supporting all economic sectors (education, transport, energy, health and security)[1]. In this respect, threats and risks associated with IoT devices and systems can have huge economic and physical consequences. As the number of IoT devices grow, so does the number of attacks and threats associated with them. According to Gartner, over 25% of cyberattacks against businesses will be IoT-based by 2025[2].

Therefore, the IoT domain considers a large and growing number of devices and technologies applied to all economic sectors, with an increasing number of types of cyberattacks. Building a **holistic framework for autonomous trust, security, and privacy management for IoT systems** as the one envisioned for ARCADIAN-IoT in such a diverse and everchanging context is a challenge that needs co-creation efforts joining academia, industry, IoT domain/solutions' experts, end-users, cybersecurity specialists and others.

In the context of the task 2.1 of ARCADIAN-IoT, the deliverable D2.2 describes the processes and results of understanding the trust, security and privacy management needs of three IoT domains: **A) Vigilance and emergency in smart cities; B) Grid infrastructures;** and **C) Medical IoT**. The consortium has a privileged position to build this knowledge as it includes partners that are experts and **solution providers** in the three IoT domains (LOAD, BOX2M, RGB), potential **end-users** (UNAV) and **IoT industry** partners with active **CSIRTs** (TRU). To this domain-related knowledge is added the **technical and research expertise** of the other partners (IPN, ATOS, MAR, RISE, TRU, UWS and XLAB) proposing trust, security and privacy management solutions - the components that jointly will form ARCADIAN-IoT framework. Complementing these perspectives are the legal, ethical and regulatory perspectives provided by the partner E-Lex. This complete and rich set of abilities was gathered in task 2.1 to deliver a set of use cases for three IoT solutions, relevant in three economic domains, which apply ARCADIAN-IoT framework components to ensure trustworthiness, security and privacy. This set of use cases is the main result of D2.2 (section 5).

The content of the deliverable D2.2 provides the base to several other ARCADIAN-IoT efforts, namely to the requirements specification (task 2.2), to the high-level architecture and research roadmap (task 2.3), and to the research work packages (WP3 and WP4), setting the ground as well to the implementation and validation work package (WP5).

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[2] https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

2. DESCRIPTION OF THE TAXONOMY

This section describes the taxonomy used for specifying and organizing ARCADIAN-IoT use cases, whose concepts and categorization are different from the ones used in the proposal. At the beginning of task 2.1 the taxonomy previously used was assessed and, after research and analysis, the partners agreed on changing the approach to one that is considered enhanced in terms of categorization granularity and concepts consistency.

The established taxonomy uses the ***IoT domain*** (or just ***domain***) to aggregate ***use cases***. In this context, a domain represents different areas of application of IoT technologies or IoT solutions. Examples of domains can be Medical IoT or Surveillance in Smart Cities. An intermediate category between *domain* and *use cases* was considered but found unnecessary in the scope of this project because the consortium will focus in just one solution from each IoT domain.

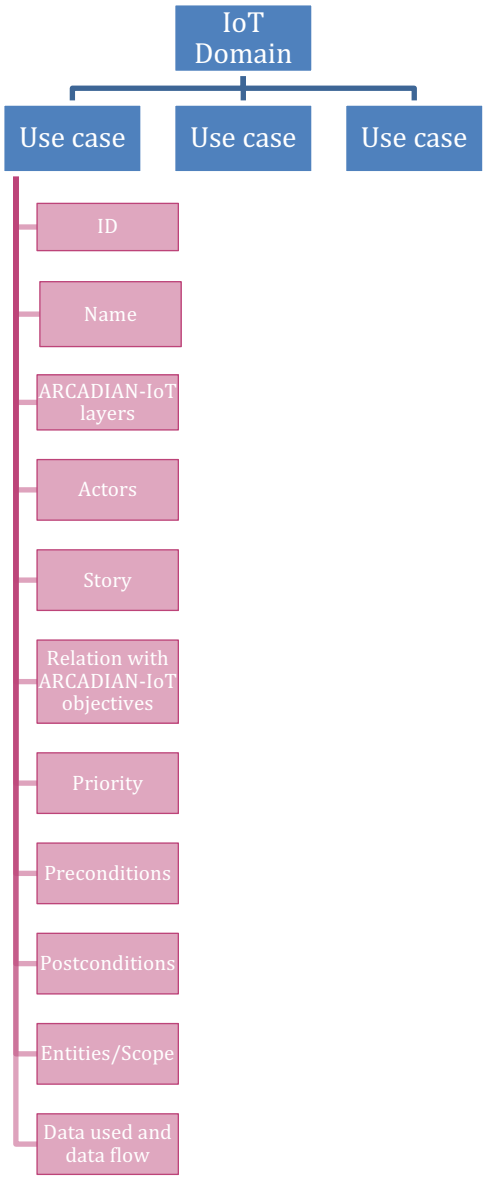

Figure 1 - ARCADIAN-IoT Use Cases Taxonomy

The *use case* is the central concept of the taxonomy (or "taxa", the taxonomic unit). Examples of use cases can be, for the Medical IoT domain, the *Patient registration* or the *Capturing and sending patient vital signs*. To ensure the coherence and meaningfulness of the specified set of use cases, and considering the unsustainable number of usage scenarios that could outcome from the work in three IoT domains, only the ones that are relevant to prove ARCADIAN-IoT concept are described (further details are provided in section 5.4). As such, a use case is specified by describing the several aspects seen in Figure 1:

a. ***ID*** is the use case unique identifier, joining the domain identifier and a sequential number.
b. ***Name*** is the use case name, designation, or title, and should clearly and briefly identify its main purpose.
c. ***ARCADIAN-IoT Layers*** relate the use case with the layers that form the project concept: in the vertical plane exist the layers of *Identity, Trust* and *Recovery*, and in the horizontal plane, the layers of *Privacy, Security* and *Common*. Each of these layers have specific components that shall be applied in the use cases where that layer is identified.
d. ***Actors*** identify the use case actors (e.g., *Patient*, or *Grid Infrastructure Manager*).

e. ***Story*** specifies, step by step, the use case. This field is quite descriptive and focuses on clearly applying ARCADIAN-IoT components in the use case flow, articulating these technologies in a coherent manner towards the future validation of ARCADIAN-IoT objectives.
f. In the ***relation with ARCADIAN-IoT objectives*** are identified the project goals that the use case will contribute to validate.
g. The ***priority*** defines the use case importance in the scale of high (*critical to several project objectives and without it some objectives could not be fulfilled*), average (*important, but other use cases have the same purpose*) and low (*nice to have, but not critical for the project objectives*). In the research process, this field allowed the partners to understand which use cases were critical and which could be avoided. Thus, considering that this document shows the final version of the research process, most of the use cases are presented as having high priority.
h. The ***use case preconditions*** state the conditions that must exist for the use case to be possible, which may include other use cases that must happen before, devices preparation, technical components status or other business-related functionalities.
i. ***Use case postconditions*** state the conditions or status that result from the use case, e.g., a user being registered, a given service started to be monitored, or a security or privacy incident is mitigated.
j. ***Entities/scope*** define which entities from the ARCADIAN-IoT concept participate in the use case (person, device, or service).
k. ***Data used and data flow*** describe the use and flow of the data in the use case, allowing to better understand the related privacy and security risks.

The categorization and concepts defined in this taxonomy were the ones used in task 2.1, in this deliverable, and are expected to be the ones used throughout the project. Continuing presenting task 2.1 organization, in the next section is described the research methodology that allowed to accomplish the task objectives.

3. RESEARCH METHODOLOGY

As previously mentioned, the nature and complexity of the challenge in hands requires effort of co-creation joining academia, industry, IoT domain/solution experts, end-users, cybersecurity specialists and others. ARCADIAN-IoT consortium has a diverse set of partners that allows to join the different perspectives required towards the targeted holistic framework. Even though, consulting external end-users and stakeholders is a valuable complement for the discovery and validation of the use cases that feed the research and, in task 2.1, the involvement of these agents has initiated.

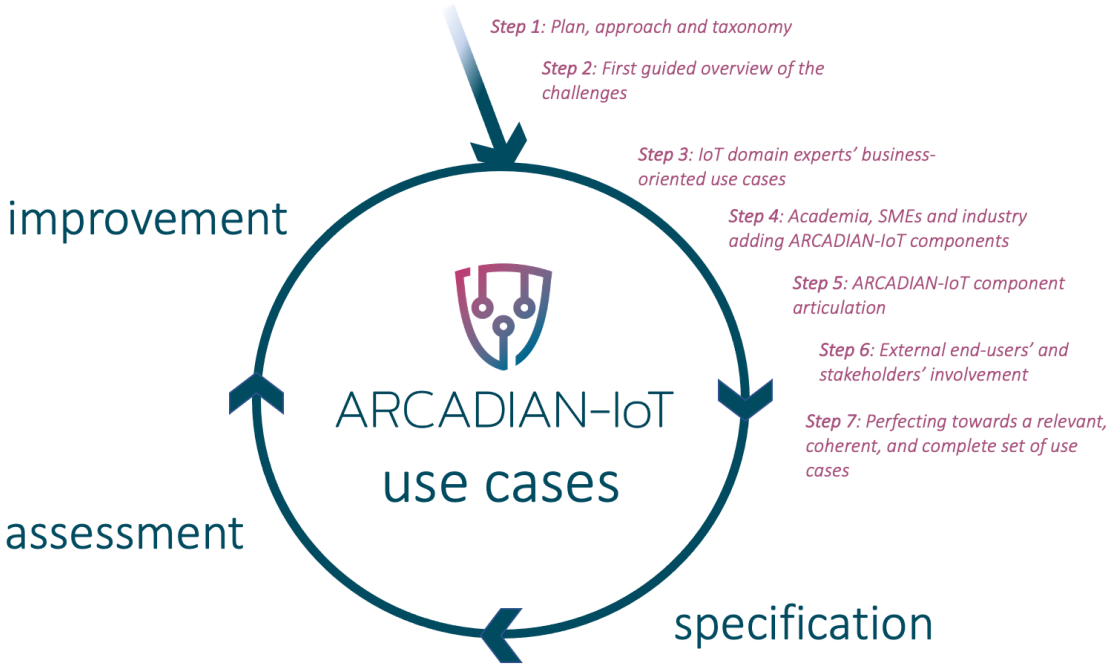

Figure 2 – Task 2.1 research methodology

Having in mind the co-creation needs and the problem complexity, the research methodology used in task 2.1 had an iterative nature, aiming for cyclically specifying, assessing and improving the use case set. The following steps describe the research methodology and techniques used.

Step 1: Plan, approach and taxonomy

The first step in task 2.1 was the definition of the plan and approach to fulfil the task objectives. Despite the iterative/agile approach, the task had a strict timeframe that needed to be considered to define the stages needed to accomplish the goals. These stages are the steps described in this section. As can be seen in Figure 2, steps 1, 2 and 3 are part of the bootstrap of the research cycle, and the other ones are iterations that comprise the **assessment** of the previous step results,

definition of the **improvement** needed or possible in that step, and the enhanced **specification** of the use case set.

Besides the general plan, the organization of the consortium on how to specify the use cases was a basilar decision that the consortium had to make at the beginning. After studying the best approaches (e.g., from other successful projects), the partners decided to change the taxonomy used in the proposal stage, as described in the previous section.

Step 2: First guided overview of the challenges

The second step of the research process, still part of the bootstrap (no use cases exist yet), was a set of workshops, facilitated by the task leader but led by the consortium IoT domain/solution experts and end-users. Having one workshop per domain, each domain expert presented, explained and answered the other partners questions about their solutions, including regarding trust, security and privacy challenges and opportunities. The workshops had as background ARCADIAN-IoT goals, as well as the use case descriptions from the proposal stage, which now start being enriched and detailed in these sessions.

Step 3: IoT domain experts' business-oriented use cases

The first description of use cases was made by IoT domain/solution experts. Naturally, this step led to a business-oriented view, with a large number of use cases per domain, full of business details, but missing solutions for trust, security and privacy management. These solutions were added in the next iterations.

Step 4: Academia, SMEs and industry adding ARCADIAN-IoT components

Building upon step 3 results, the partners experts in the components of ARCADIAN-IoT framework, started providing inputs and comments to the existent use cases. To facilitate the process of assessment of the current use cases and elicitation of new ones that were missing, the task leader provided a *Technology Articulation Map* for each domain (final results of this technique in section *5.4 Use cases verification*). This technique comprised one matrix per domain that allowed to describe, for each domain, which ARCADIAN-IoT components participate in each use case. With this exercise, it was easy to identify that, for example, components from the identity vertical layer of the framework had direct participation in use cases of registration, login, and identification of persons, devices and services.

In another iteration of this step, having the overview of the use cases and of the related ARCADIAN-IoT components usage, were visible some missing spots, detected when a partner responsible for a component was not able to find any use case to contribute to. This happened, for example, in components of the security horizontal layer of the ARCADIAN-IoT concept, often forgotten in the business-oriented use cases. This knowledge gave partners the opportunity to propose new use cases, enriching the initial IoT solutions with the framework's security, trust and privacy management features.

The *Technology Articulation Map* made also clear that some use cases, although relevant for the IoT businesses, had unclear purpose within the project goals, given that no component had an envisioned participation. These ones were kept in the *Technology Articulation Map* until the step 7, where there was made a move to the final set of use cases, which had to be relevant, coherent, and complete, considering not only the business perspective, but also the project objectives.

Every move in the use cases was made in co-creation between the technical partners, IoT domain/solution experts and end-users. This co-creation was materialized in meetings about the topic every two weeks, the use cases set described in preliminary versions of D2.1 and the *Technology Articulation Map* shared and available online to all.

Step 5: ARCADIAN-IoT components articulation

The knowledge built in the previous step made also clear that some components had simultaneous participation in the same use cases, which raised the need for having further effort towards component articulation. For this purpose, one-to-one meetings between partners with directly related components were encouraged and held, resulting in an enhanced clarity to the research hypothesis and on improvements to the existent use cases.

Step 6: External end-users' and stakeholders' involvement

Having a good preliminary understanding of the problems and of potential solutions described in preliminary use cases, partners decided to validate that initial knowledge and understand external end-users' and stakeholders' perspective. To this end, were built four surveys targeting users from the different IoT domains of the project. Specifically, the surveys were built for the following end-users:

i. Regular citizens, potential users of drone-based vigilance and emergency services
ii. Grid infrastructure owners/managers
iii. Medical doctors and other staff responsible for patient monitoring
iv. Regular citizens, potential patients using medical IoT solutions for health monitoring

There was a fifth survey targeting cybersecurity professionals (e.g., CSIRT members).

This initiative involved all the partners from task 2.1, who provided questions that allowed to validate their components / technology and better understand their requirements. EUSurvey[3] platform was used to set up the surveys. Legal and ethical GDPR concerns were addressed by the consortium legal partner (E-Lex), ensuring compliance with legal, ethical, regulatory and social dimensions. The surveys and related plan to approach end-users were analysed, validated, and approved by the project Technical Committee and Advisory Board. Results were consolidated and analysed, allowing to validate the envisioned use cases accordingly. The surveys used and their consolidated results are presented in *Appendix A*, and a summary of the key findings can be found in section 5.4.1.

[3] https://ec.europa.eu/eusurvey/home/welcome

Step 7: Perfecting towards a relevant, coherent, and complete set of use cases

Finally, based on workshops that gathered all participants of task 2.1, one extended session per domain, the last step consisted of perfecting the set of use cases towards meaningfulness, completeness, and coherence. Only the use cases that are relevant for the project objectives validation were kept, ensuring as well that all the project objectives could be validated with the existent set. To ensure business-wise relevance of the use cases, pertinent business features not related with security, trust or privacy management were added as post-conditions or pre-conditions of the final use cases.

As result, patterns of usage and articulation between ARCADIAN-IoT components across the three domains are visible in the use cases' description (to be formalized in D2.5). These patterns indicate that the consortium not only achieved a seamless application of the trust, security and privacy management features in the project specific cases, but also started to define a tangible framework where the components are agnostic to the IoT domain and prepared to be used in other IoT contexts.

Due to task 2.1 schedule, step 6 and 7 happened simultaneously. Furthermore, the research process initiated in this task is planned to be continued in WP5, particularly in task *5.5. Use cases technical and legal compliance validation*.

After depicting the taxonomy used and the research methodology, in the next section are presented the domains of application of the technologies target of research in the project.

4. DOMAINS' DESCRIPTION

This section describes overall stories related with each IoT domain that will be used to demonstrate ARCADIAN-IoT framework, anticipating and introducing the context for the use cases specification. Being a business-oriented description, it allows to have a clearer vision regarding the solutions' functionalities, but also of the security, trust and privacy management challenges, which will be targeted in the use cases described in section 5.

4.1. Domain A: Emergency and vigilance using drones and IoT

Ensuring security and safety of citizens in urban environments is a complex subject that depends on the availability of considerable resources, with high costs, and, in many cases, the use and manipulation of sensitive data (e.g., when using street vigilance cameras communicating with centralized data centers). ARCADIAN-IoT domain A focuses on the use of IoT devices, in this case, drones, in novel efficient and citizen centered urban vigilance services.

Illustrating a potential story of this IoT solution, high-level scenarios can feature a young lady, Ana, who is on her way home alone, after a dinner with friends. Using ARCADIAN-IoT Drone Guard Angel (DGA) app in her personal device, Ana requests vigilance services to escort her home. The service is available in her city and, to be registered and recognized by a DGA, Ana has supplied some personal data in the registration phase, like name, address and photos. When requesting the service, she needs to provide her initial and final location, to ensure that the service is available in both spots.

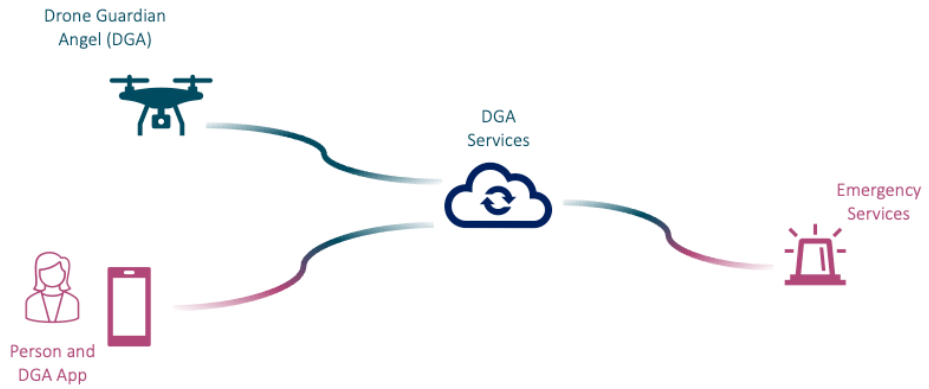

Figure 3 - DGA participant entities

After receiving the service request with Ana's data (e.g., location and identification), a drone parked in a specific place in the neighbourhood lifts off and arrives near her. The first thing it does is to validate the user through multiple criteria, which includes the recognition of Ana's smartphone and her physical characteristics (e.g., face recognition). After the successful identification, the drone notifies her that it is ready to guard her home.

Ana starts walking home and the DGA is following her, aware of the surroundings for detecting any threat signal (e.g., rapid movements towards Ana, high speed vehicles or objects). If something abnormal is detected (e.g., an attempt of robbery), the drone can start an appropriate manoeuvre to scare or demotivate the robbers (blinking lights, emitting sounds, etc.), while it calls for rescue (police). If injuries are detected, a medical rescue team is also called. While the rescue team(s) is/are on its way, some details can already be sent, collected by the camera, microphone and appropriate sensors (e.g., GPS), to give precise location and provide the incident characteristics (e.g. number of people involved or type of injuries).

Trust, security and privacy management challenges

DGA solution relies on an IoT device to provide its service to persons, who should have a personal device (smartphone) to use the service. Depends as well on the use of persons sensitive data, like location, address, and photos for facial recognition. In this sense, trust, security, and privacy management challenges arise, namely:

- Enable security and trust in the management of drones' identification, ensuring protection to, e.g., impersonation attacks that could endanger the person physical and data security.
- Enable security and trust in the management of persons' identification, ensuring protection of the user ID data (e.g., biometric data and ID credentials), used by the IoT devices and DGA services.
- Define trust evaluation models for the DGA devices, services and app, where the end-user is aware of the trustworthiness of the system components and of his data privacy (who accesses what and when). These trust models also allow the framework to adapt autonomously to compromised components.
- Protect the users' and devices sensitive data (authentication credentials, location, course/path, photos) with hardened encryption mechanisms with recovery ability.
- Detect anomalous behaviour on IoT devices (drones) and related services, which can indicate the presence of known or zero-day vulnerabilities or threats.
- In case of an incident with a drone or a personal device DGA ecosystem (e.g., app services and related data), have autonomous self-recovery mechanisms that allow to recover functionalities and data to pre-defined trust levels with reduced human intervention.
- Enable an automated and privacy-preserving cyber threat intelligence (CTI) approach for IoT threat information generation, sharing, analysis, storage, and consumption.

The use cases provided in section 5.1 aim to show how ARCADIAN-IoT addresses the aforementioned challenges.

4.2. Domain B: Secured early monitoring of grid infrastructures

Grid infrastructures are the base for power utilities like electricity, gas or oil. These are critical services for the daily activity in urban environments, namely at homes, factories, workplaces, and in public services, like the ones of health or safety. Monitoring these infrastructures assumes high importance for providing consistent and reliable services, ensure efficient energy management practices, namely with smart metering integration, automation, and precise decision support systems. IoT technologies, namely sensor technologies and wireless solutions open the door to these novel features that depend on advanced monitoring of the grid infrastructures components. Such an IoT ecosystem allows to identify relevant operational aspects like changes in substations (e.g., temperature, humidity, and other environmental aspects), discharges, levels of oil and gas, or component degradation. These variables identification is critical to act accordingly, automatically or with decisions supported by up-to-date information.

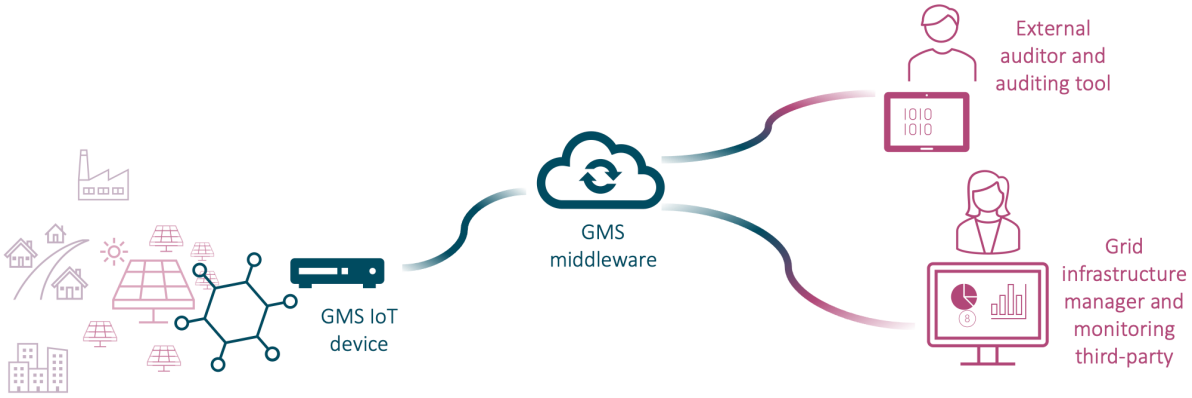

Figure 4 - GMS participant entities

ARCADIAN-IoT domain B features an IoT solution for monitoring grid infrastructures. As a potential scenario of application, it is possible to illustrate a renewable energy harvesting site, particularly a solar energy harvesting site, which, being connected to the city electricity grid, is providing 60% of the power needed for the houses of 200,000 citizens. The grid infrastructure manager needs to be aware, for example, of the performance of each photovoltaic panel and each heat storage unit. Also needs to understand factors that influence and allow to optimize and predict the energy harvesting, like temperature, irradiances, humidity, wind speed and others. The installation has also operation circuits for cooling and heating fluid, and several critical valves whose degradation needs to be monitored to minimize the stopping the service due to malfunction. The ARCADIAN-IoT Grid Monitoring Services (GMS) features a solution that collects and aggregates data from a set of sensors installed - an **IoT device** built and provided by BOX2M that acts as gateway for the grid sensors. This IoT device puts that data available, through a **middleware**, to be consumed by grid managers in a web or mobile monitoring service. GMS also allows a grid manager to change the sensors procedures (e.g., change the reading cycle frequency). Finally, the solution is prepared for external audits, where data from devices/sensors needs to be securely provided to authorized external persons.

Trust, security and privacy management challenges

GMS solution collects grid infrastructure data from a set of devices that inform about renewable energy harvesting status and related factors. The trustworthiness of this data is critical because otherwise it can lead the system or the manager to wrong decisions, or even put at risk the energetic needs of a city's businesses and citizens. This is also confidential business data, that can harm the service provider if accessed by unauthorized parties. Furthermore, GMS provides means to interact with the sensor network, action that needs to be secured to avoid illicit accesses to it. The third-party monitoring tool can also be targeted in network attacks, e.g., DDoS, making the service unavailable and delaying/hampering potentially relevant decisions or power provisioning. In this sense, trust, security, and privacy management challenges arise, namely:

- Enable security and trust in the management of devices identification, ensuring protection to, e.g., impersonation attacks that could endanger the business assets physical and data security, or feed fake data into the system, leading to the whole service malfunction.
- Enable security and trust in the management of persons' identification, ensuring protection of the grid manager and other authorized people identification, used to access the IoT devices data and control their functionalities, and protection to unauthorized accesses to the GMS services.
- Define trust evaluation and management models for the IoT devices and GMS services, allowing the grid manager to be aware of the trustworthiness of the system components and of the infrastructure data privacy, and allowing the framework to adapt autonomously to compromised components.
- Protect the devices sensitive data (environment sensor readings, components degradation, discharges) with hardened encryption/decryption mechanisms with recovery ability.
- Allow external entities to audit the grid infrastructure without endangering the data privacy and security.
- Autonomously detect anomalous behaviour on IoT devices and related services, which can indicate the presence of known or zero-day vulnerabilities or threats.
- In case of a security or privacy incident with the GMS IoT device or the service itself, have autonomous self-recovery mechanisms that allow to recover functionalities and data to pre-defined trust levels with reduced human intervention.
- Enable an automated and privacy-preserved CTI approach for IoT threat information generation, sharing, analysis, storage, and consumption.

The use cases provided in section 5.1 aim to show how ARCADIAN-IoT addresses the aforementioned challenges.

4.3. Domain C: Medical IoT

Monitoring patients at their homes, when possible, is important for the sustainability of health systems and for the comfort of the monitored persons. IoT systems, namely body sensor networks, provide solutions that make this possible. However, the use of IoT solutions for medical purposes raise concerns, such as those related to the patient's data privacy and security.

ARCADIAN-IoT Medical IoT (MIoT) scenario can be described as follows: The tumour was first removed from Maria (5 years old) in Ecuador, and she is now being treated in Madrid. It is a very rare cerebral sarcoma with a poor prognosis, associated with DICER, a rare genetic disorder that predisposes individuals to multiple cancer types. The paediatrics radio-oncology treatment is based on a proton medical device that generates, during the required number of sessions (e.g., 30), intensive radiotherapy by sending large amounts of proton to the brain tumour. Almost all patients receive radiotherapy and chemotherapy, but each of them undergoes different treatments and is treated in a personalized manner.

Considering the demanding volume of treatment sessions, reducing the number of consulting sessions for assessing the patient's well-being is very beneficial. For this purpose, a telemonitoring system is well accepted by the medical staff - team of doctors and nurses - and by the patients. Both see the solution as more comfortable and able of automatically providing an evolutionary record of the patients' status, and potentially getting the medical staff attention to relevant readings. This is the context for the application of ARCADIAN-IoT MIoT solution.

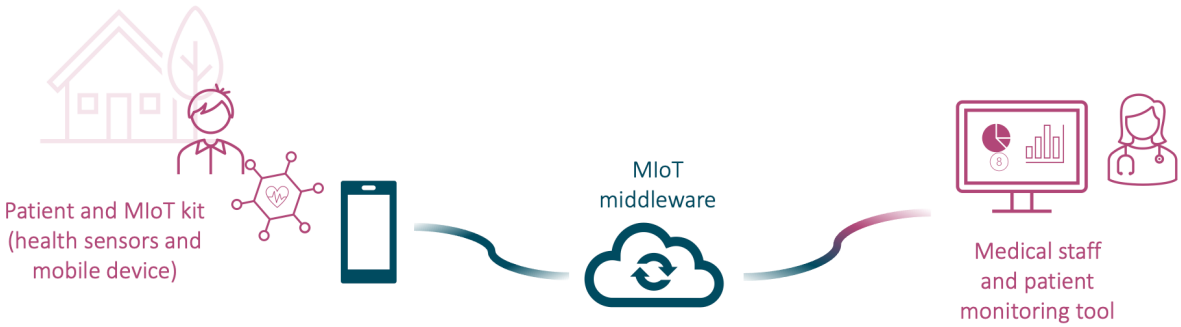

Figure 5 - MIoT participant entities

According to medical experts (UNAV, ARCADIAN-IoT partner), to be effective, MIoT needs to be able to monitor patients considering a treatment protocol (readings frequency, medication, and other medical recommendations). It needs to collect, store, and present the evolution of vital signs, namely in the cardiac area, the heart rate, temperature, SpO2 and blood pressure, captured with the medical sensors and timely provide alerts for medical decision support. To complement these parameters, it should be possible for the patient to enter perceived symptoms in a mobile app, such as levels of fatigue, sweating, diarrhea, or others that can describe a symptom intensity.

To fulfil these requirements, the solution will rely in a MIoT kit that comprises a set of medical sensors, and a smartphone that will be used as gateway for the sensing devices and as interface for the patient to enter his/her perceived well-being. This kit is provided to the patients at the hospital. The solution will also include a MIoT middleware service for distributing securely the patients' data and generating health alerts; and a monitoring tool for the medical staff to check the patient's well-being, alerts and to change the monitoring protocol when needed.

Trust, security and privacy management challenges

ARCADIAN-IoT MIoT solution aims to improve the conditions of monitoring and follow-up of cancer patients at home, in the active treatment process where patients complement the sensorial data with their perceived well-being. However, by collecting patient's data from a set of devices that inform about the person health, and the perceived well-being collected with a mobile app, the system deals with sensitive information. The trustworthiness of this data is critical for the medical staff to make right treatment decisions. Fake or manipulated diagnostic information can put the patients' well-being, or even their lives, at risk. This data is also confidential and can't be accessed by unauthorized parties. Furthermore, MIoT provides means to update the patient monitoring protocol, communication that needs to be secured to avoid illicit access or control over the data or devices behaviour, which can harm the patient. The mobile app and the monitoring tool for the medical staff can also be targeted in network attacks, e.g., DDoS, making the services unavailable and delaying/hampering potentially relevant medical decisions. In this sense, trust, security, and privacy management challenges arise, namely:

- Enable security and trust in the management of devices identification, ensuring protection to, e.g., impersonation attacks that could endanger the physical and data security of the patients, e.g., by feeding fake data into the system.
- Enable security and trust in the management of persons' identification, ensuring protection of the patient and medical staff identification, which could lead to unauthorized access to private data and control of the devices.
- Define trust evaluation and management models for the MIoT devices and services, allowing the end-users to be aware of the trustworthiness of the system components and of their data privacy, and allowing the framework to adapt autonomously to compromised components.
- Protect the devices sensitive data with hardened encryption/decryption mechanisms with recovery ability.
- Detect anomalous behaviour on IoT devices and related services, which can indicate the presence of known or zero-day vulnerabilities or threats.
- In case of a security or privacy incident with the IoT devices or the service itself, trigger self-recovery mechanisms that allow to recover data and at least 95% of the system functionalities prior to anomalous behaviour. Support coordination of recovery to pre-defined trust levels with reduced human intervention.
- Enable an automated and privacy-preserved CTI approach for IoT threat information generation, sharing, analysis, storage, and consumption.

Considering the context and challenges of the three IoT domains presented, in the next section are depicted the specific use cases that apply ARCADIAN-IoT technologies in these realities, attempting to mitigate the existent challenges.

5. USE CASES SPECIFICATION AND VERIFICATION

Considering the contexts introduced in the previous section, here are described use cases that depict the envisioned application and incorporation of ARCADIAN-IoT framework in solutions to ensure trust, security and privacy management in those three IoT domains:

- Domain A: Emergency and vigilance using drones and IoT
- Domain B: Secured early monitoring of smart grid infrastructures
- Domain C: Medical IoT

Given that ARCADIAN-IoT aims to be a holistic framework most of its components should apply to different contexts and different domains, even beyond the three ones targeted for demonstration in the project. The different settings analysed in this work allow the consortium to start envisioning the agnostic technologies needed, and the reader will be presented with the use of each ARCADIAN-IoT component in more than one context. Moreover, the trust, security and privacy management solutions needed to cope with the challenges depend on articulation processes between components. Patterns of articulation between ARCADIAN-IoT technologies will be visible in the use cases' description but will just be formalized in task 2.3 (D2.5), where the framework architecture is described.

The use cases presented considered each domain characteristics and were selected based on the perceived relevance to solution providers and end-users, but also to allow to demonstrate (in WP5) ARCADIAN-IoT objectives. Each use case will be described considering aspects like the ARCADIAN-IoT layers that apply and the project objectives targeted, the actors, the use case story, the data used and the data flow, and others (taxonomy in section 2). These aspects will allow to assess the set of use cases coherence, relevance and completeness in section 5.4.

5.1. Domain A: Emergency and vigilance using drones and IoT

For domain A the following use cases were selected:

- A1: Person registration at DGA service
- A2: Person authentication at the DGA service
- A3: Person retrieving and editing personal data
- A4: Person requesting a DGA service
- A5: DGA service
- A6: Drone security or privacy incident
- A7: Personal device security or privacy incident

5.1.1 Use case A1: Person registration at DGA service

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
The first step for using ARCADIAN-IoT Drone Guard Angel (DGA) is the person registration in the service. To do so, the person, e.g., a regular citizen, uses a **compliant mobile app**[4] previously downloaded and installed in his/her smartphone. The DGA service trustworthiness is provided to the user before registration, and the personal device is prepared to integrate ARCADIAN-IoT, namely with the **eSIM** as Root of Trust (RoT), mechanisms for **hardened encryption**, for integrity **attestation**, and with a **self-sovereign identity** (SSI like **decentralized identifier** or **verifiable credential**). The person provides the necessary data (including biometric information), which is encrypted with RoT, for registration in the services. At least 3 robust identity mechanisms, one of which decentralized and other secure at hardware level, are provided to the person. ARCADIAN-IoT framework sets up the mechanisms for security and privacy monitoring, and for recovery in case of an incident, for that particular person/personal device. The person is kept informed and with control over where its data is used (**self-aware data privacy**).

[4] Definition of the requirements for being an ARCADIAN-IoT compliant mobile app is presented at D2.4

Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. DGA services are compliant with ARCADIAN-IoT. 2. User has a smartphone with eSIM and the DGA app installed. 3. (starts with the user acceptance of the terms provided within this use case) ARCADIAN-IoT behaviour monitoring component monitor the interactions of the user, personal device, and third-party service to - in articulation with the CTI component - trigger any security action needed and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. The user is registered in the system, has at least 3 strong identification mechanisms configured, being one of them decentralized, and the RoT on his/her personal device has information for performing hardened encryption of the private data. The user is able to securely log in and start using the services of the ARCADIAN-IoT third-party, the DGA services, with his/her sensitive data privacy ensured. 2. The ARCADIAN-IoT third-party (DGA services), has the necessary data for providing its service.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.
Data used and data flow
1. Information for hardened encryption is provided to or generated at the RoT of the user personal device. Information for decrypting user data is securely sent to ARCADIAN-IoT third-

party services, when needed. The person authorizes the services to access his/her data. Personal data not in use is always kept encrypted. 2. User personal data needed for the SSI (Verifiable Credentials / Decentralized Identifiers) to be defined in the research process. Its flow will start in the user personal device, where it is encrypted and sent to ARCADIAN-IoT services. With the person authorization, data is decrypted and used for the decentralized ID generation, being placed in a permissioned blockchain for restore in case of need. The necessary personal identification data is returned to the user and stored in a secure ID wallet or in the RoT. 3. Biometric material is generated in the user mobile device, encrypted with RoT information and sent to the compliant ARCADIAN-IoT third-party services.
Main implementation risks or uncertainties
1. Store credentials and encryption keys securely at the device RoT, and implement a novel hardened encryption mechanism. 2. Generate and join decentralized identifiers with cellular network credentials for person authentication in third-party services. 3. Implement a trust model based on reputation that allows the users to know the compliant services trustworthiness. 4. Bootstrap all ARCADIAN-IoT processes related to a new user, namely for recovery in case of need.

5.1.2 Use case A2: Person authentication at DGA service

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane:** Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
When registered, the user needs to authenticate himself/herself with **more than one robust identity mechanisms** to access ARCADIAN-IoT DGA services. For this authentication step in the app will be used **new SSI and cellular network credentials identification** mechanisms. ARCADIAN-IoT trust models (informed by **monitoring and CTI** components) will be in place to allow or refuse the person / device / app authentication.

Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use case A1. 2. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the user, personal device and third-party service in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. The user is logged in in ARCADIAN-IoT DGA and may request a service.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.
Data used and data flow
1. The ARCADIAN-IoT compliant app requests the authentication data from the RoT and/or an ID wallet. If the app is trustable and access is given, data is retrieved from the secure element to the device and the flow continues from the user personal device to DGA services. In these services, the ARCADIAN-IoT authentication process happens with more than one authentication factor and, if successful, information about that is securely returned to the device authorizing the user to proceed.
Main implementation risks or uncertainties
1. Use of SSI and network credentials to access third-party services. 2. Have a custom authentication service that uses the intended several factors to authenticate the person in the compliant third-party.

3. Implement a trust model based on reputation to be the source of an authorization component (authorization to login in DGA services in this case).

5.1.3 Use case A3: Person retrieving and editing personal data

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane:** Privacy; Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
The end-user can retrieve and edit his/her personal data (registered in the system) using DGA mobile app. DGA services validate the **user, device and app identity and trustworthiness**. If the entities are authorized and trustworthy, the data is retrieved **encrypted** and decrypted at the device, with private cryptographic material kept secure at hardware level, for editing. After the intended edition, it is **encrypted again with RoT information** and sent to DGA services, where it is kept encrypted until the user authorizes any access to it (**self-aware data privacy**).
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.

Use case preconditions
1. Use cases A1 and A2. 2. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the user, personal device and third-party service in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. Updated personal data stored, encrypted, in DGA services.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.
Data used and data flow
1. If the requesting entities are trustable and authorized, personal data (e.g., name and address) is retrieved, encrypted, from DGA services to the requesting mobile device. It is decrypted with private cryptographic material. After editing the data is encrypted again and sent to DGA service. It is not stored decrypted anywhere (not at the device nor at the Cloud).
Main implementation risks or uncertainties
1. Implement a trust model that uses reputation and validate all the entities trustworthiness before sending the requested data. 2. Perform hardened encryption and decryption with RoT information.

5.1.4 Use case A4: User requesting a DGA service

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
A central functionality of the ARCADIAN-IoT DGA services takes place when the end-user requests a drone using the DGA mobile app. In this case, the user requests, from ARCADIAN-IoT DGA services, a drone to a desired service location, sending the necessary personal data **encrypted with RoT information** (location and an image of the face in the current conditions

may be needed). After verifying the user's identity, location, and the requesting app and device trustworthiness (via the **reputation** system), ARCADIAN-IoT DGA service select a drone from the available ones – the drone itself is selected considering that **IoT device reputation** information. The selected drone identity data is retrieved from its hardware (RoT) and **attested**, assuring the device trustworthiness (no impersonation) before granting it access to the user's personal data. ARCADIAN-IoT DGA services share the necessary data (location, biometric data), **encrypted**, with the drone. The device, if trustworthy, it is able to decrypt the data with RoT information, allowing it to meet the person and attest its identity. The person is informed that a trustworthy drone has its location and identification for performing the service (self-aware data privacy). Drone's identification may be shared with the person if relevant, for a visual identification upon the devices' arrival to the service location.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use cases A1 and A2. 2. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the user, personal device and third-party service in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. Use case A5.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.

Data used and data flow
1. The data used is the personal data needed for the DGA service, e.g., location and photo. The data flow starts at the user personal device, when the personal data needed is encrypted and sent to the DGA services. After security /trust validation of the parties involved, DGA services share the data (still encrypted) with the IoT device (drone). If trustworthy, the device is able to decrypt the data and use it to proceed with the service.
Main implementation risks or uncertainties
1. Selection of IoT device, drone, for service, based on its trustworthiness / reputation. 2. Perform attestation of IoT device before granting it personal data. 3. IoT device decrypting service data with RoT information.

5.1.5 Use case A5: DGA service

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
After being granted with a service and having the necessary data, a drone needs to meet and identify the person that requested it and proceed with the vigilance service. The person is informed about the selected device **reputation,** and how to perform the needed **biometric identification**. When the person is near the drone, a process of IoT devices **mutual authentication** (person personal device and drone) happens. All the private data exchanged is encrypted and only accessible by the targeted devices. In this case are used **3 multiple simultaneous identification** of the person. If the identification process is successful the service starts, and the drone starts following the person. Any user data sent by the drone to DGA services, including from emergency or rescue, is encrypted and only accessible by entities (previously) authorized by the user. When the service ends, all the user personal data is deleted from the drone, and any data needed in DGA services about the user or the service is kept encrypted. The user is informed of which data is kept in the service and may choose to delete it.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use case A4. 2. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the user, personal device and third-party service in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved. 3. Processes of anonymization of people nearby the user are in place.
Use case postconditions
1. If the service ends successfully, the drone returns to the base with no other action needed. 2. If for some reason the service doesn't end successfully, the behaviour monitoring and the CTI try to infer the reason and act accordingly. DGA services perform the corrective measure considered needed (e.g., an operator calls the user, or the services send another drone to the last known location to continue the service or assess the situation).
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.
Data used and data flow
1. At the beginning of this use case, a drone has the user personal data required to perform the service, data that it was able to, being known as a trustworthy device, decrypt to proceed with the service. 2. After arriving the user location, both the drone and the user personal device send their location and mutual authentication material, encrypted with RoT information, to the DGA services. 3. If successful, the drone captures the user biometric data (images or video), encrypts it and send it to DGA services for applying AI models for person biometric identification. Biometric data is decrypted in DGA services and processed to ascertain if the identity of the user is valid for the service to start. The other components of the user identity remain anonymous to the AI service, which just receives images/content to compare. If the result is positive (and the other

identification processes also), the service starts and the drone and personal device behaviour is monitored (encrypted service data being sent to DGA services). 4. Abnormal events are also being monitored, by the service provider. If an abnormal event happens, encrypted data about it is sent to DGA services for an authorized operator to act upon. 5. At the end of the service all the user personal data is deleted from the drone. Data about the service may be kept encrypted in DGA services, with the user awareness. The person may request the deletion of the data about the service from DGA services.
Main implementation risks or uncertainties
1. Person biometric identification using drones' hardware – data processing location (drone or cloud) is topic of research. If in cloud, anonymization process for the images/content will also be topic of research. 2. Mutual authentication between personal devices and drones. 3. Behaviour monitoring of all the entities involved, processing cyber threat intelligence and automatically adjusting entities reputation when necessary.

5.1.6 Use case A6: Drone security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Attacker(s).
Use Case Story
This use case depicts the scenario of a drone security or privacy incident. It includes the device preparation for it (for incident **detection** and **recovery**), the private data and identity **protection**, including procedures of self-protection, and the subsequent actions of **recovery**. Examples of security or privacy incidents are the cases where the IoT device is stolen, has unauthorized access to the private data it owns, or unauthorized control or manipulation of its behaviour. For being able to detect, protect and recover from a security or privacy incident, at every moment of the operational life of the IoT device, the drone in this case, information is being securely collected by an ARCADIAN-IoT component, like the **behaviour monitoring**, and interpreted by a **cyber threat intelligence (CTI)** tool, which is kept updated with the known IoT threats and aware to zero-day threats/vulnerabilities (inferred e.g. from behaviour monitoring and rules for new potential threat detection). Also, for this purpose, a **federated AI** paradigm will be in place for collectively training an AI model on distributed information while ensuring **data privacy** and informing the device **self-protection** mechanisms.

For **protecting** the end-users' private information, the data is kept **always encrypted** and just sent to the drones after a security assessment made to the device (**attestation**). Also, a dynamic **reputation** system defines the device trustworthiness according to the several factors, including its previous **behaviour**, which is being monitored and interpreted. Only trustworthy devices receive vigilance services and the related data, including cryptographic material for decrypting private data. Hardware measures at compromised devices for blocking attacks will also take place[5]. Moreover, its communication capacities are kept under control with a network-based **authorization** enforcement tool, which is always aware of all devices' **reputation**.

Regarding the IoT device identity, to ensure its **protection**, it is composed of several factors to be used simultaneously, being at least one stored in the hardware secure element – **eSIM**/eUICC (the **network credentials**), and a second one a **decentralized identifier**, not controlled or stored at any centralized entity. The network credentials manipulation and the RoT (**eSIM**) over-the-air communication with the network happen according to the well-accepted and widely used GSMA security accreditation schema (GSMA-SAS).

In the case of a security incident being detected, the device **reputation** is updated accordingly immediately, and the internet accesses **authorization** enforcement as well. With this, the device can only access services for **recovering** from the incident. Has no access to services that may provide private data or cryptographic material nor has access to external services that may be controlling it or gathering the device private data. If the device is operational and cooperative, it takes actions for recovery from the incident according to the type (**self-recovery** component). Self-recovery procedures are defined and require access to ARCADIAN-IoT services, and the **authorization** enforcement component (placed at the network provider core elements – between the device and the internet) assures that these are the only ones available to the compromised device.

If or when the **self-recovery** processes are successful, the device software and hardware is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. Network credentials can be recovered with the network operator. The decentralized identifiers can be recovered from the ARCADIAN-IoT **blockchain** component.

Along the process, the **cyber threat intelligence** tool shares threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

Objective 6: Self and coordinated healing with reduced human intervention.

[5] Details removed for potential IPR protection

Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Drone is compliant with ARCADIAN-IoT[6]. 2. Related ARCADIAN-IoT framework components (e.g., reputation system, authorization, self-protection, self-recovery) are operational.
Use case postconditions
1. If the device is operational (e.g., didn't got damaged), not stolen and cooperative, the incident is mitigated and its security and privacy is restored. 2. Anonymized data / trained models about the incident are shared with CSIRT and CERT.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
IoT device and Services.
Data used and data flow
1. Evidence of drone's behaviour is collected on the device operation. 2. Periodically information to attest the device identity is also gathered. 3. Typically, no sensitive data is collected, although, given this IoT device particular operation, location may be part of the collected data, to infer its behaviour. However, this data is not associated in ARCADIAN-IoT with any drone service (no relation with the particular person requesting the service). 4. Behaviour data is interpreted by CTI and federated AI components to infer threats or incidents. 5. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to reduce the device reputation and update, as soon as possible, its authorization of communication accordingly. 6. In the case of a compromised device, that drone hardware will take measures to block/protect the device and its data from the attack[7]. 7. In a recovery process, decentralized credentials are recovered from the blockchain component, and network credentials are recovered from the network operator.

[6] IoT devices compliance with Arcadian-IoT defined in D2.4
[7] Details removed for potential IPR protection

8. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.
Main implementation risks or uncertainties
1. Drone behaviour monitoring and attestation. 2. Threat detection (CTI) and learning (federated AI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection. 4. Identity protection combining several identification processes. 5. Automatic combination of CTI and drone attestation with its reputation. 6. Drone reputation models articulated with connectivity authorization enforcement. 7. Articulation of network-based authorization enforcement hardware-based threat protection. 8. Decentralized credentials recovery using blockchain. 9. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.1.7 Use case A7: Personal device security or privacy incident[8]

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane:** Privacy; Security; Common.
Use Case Actors
Attacker(s).
Use Case Story
This use case depicts the scenario of a personal device security or privacy incident that endangers DGA services and its related data (personal and sensitive). It encompasses the device preparation for the incident **detection** and **recovery**, the **protection** of the private data and identity of the owner and of the device itself, and the subsequent actions of **recovery**. Examples of security or privacy incidents are the cases where the personal device is stolen, has unauthorized access to private the data it owns, or unauthorized control or manipulation of the device behaviour in what concerns DGA services. For being able to **detect, protect** and **recover** from a security or privacy incident, after the person registration in the DGA app, security information starts being collected by ARCADIAN-IoT, e.g., by the **behaviour monitoring** component, and interpreted by the **cyber threat**

[8] For the purpose of this use case, the personal device ecosystem should be understood as comprising (1) the DGA app and the related data stored and/or processed in the device; (2) the device RoT hardware and software– eUICC/eSIM – and any middleware for communication between the device and its RoT; (3) the ARCADIAN-IoT components that live in the device. The personal device ecosystem considered in this use case doesn't consider breaches in any other app or mobile service not compliant with ARCADIAN-IoT.

intelligence tool. Also, for the same purpose, a **federated AI** paradigm will be in place for collectively training an AI model on distributed data while ensuring the **data privacy** and supporting other components, e.g., of device and data protection and threat analysis.

For protecting the person private data in case of an incident, sensitive data present in the device is kept **encrypted with RoT information**. A dynamic **reputation** system defines the device and DGA app trustworthiness according to the several factors, including its behaviour, which is being monitored and interpreted, and an **attestation** component that seeks breaches in the device integrity. The hardware will have in place mechanisms for protecting the sensitive information from compromised devices[9]. Also, its communication capacities will be kept under control with a network-based **authorization** enforcement tool, which is always aware of devices' and services' **reputation**.

Regarding the person and the personal device identity, to ensure its security, it is composed of several factors to be used simultaneously, being at least one stored in the hardware secure element – **eSIM**/eUICC (the network credentials), and a second one an SSI (e.g., a **decentralized identifier**), not controlled or stored at any centralized entity. The network credentials manipulation and the communication with the device RoT happens according to the GSMA security accreditation schema and can be recovered with the network operator. The SSI can be recovered from the ARCADIAN-IoT **blockchain** component.

In the case of a security incident being detected, the personal device **reputation** is updated accordingly immediately, and the accesses **authorization** enforcement as well. With this, the device DGA app can only access services for **recovering** from the incident. Has no access to other ARCADIAN-IoT services, that would allow, for instance, to request drones or attack related services. If the device is operational and cooperative, it takes actions for recovery from the incident according to the type (**self-recovery** component). Self-recovery procedures are defined at, and may require access to, ARCADIAN-IoT services, and the authorization enforcement component (placed at the network provider core elements) ensures that these are the only ones available to the compromised device until it recovers from the incident.

If or when the **self-recovery** processes are successful, the device software and hardware is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. The human intervention is reduced to the strictly necessary in healing and recovery procedures.

Along the process, the **cyber threat intelligence** tool shares threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

[9] Details removed for potential IPR protection

Objective 6: Self and coordinated healing with reduced human intervention. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Personal device is compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., CTI, reputation system, authorization, self-protection, self-recovery) are operational.
Use case postconditions
1. If the device is operational (e.g., didn't got damaged) and not stolen, the incident is mitigated and its security and privacy is restored. 2. Threat information in the form of trained models is shared with CSIRT and CERT networks for propagating the threat awareness.
ARCADIAN-IoT Entities (Person/ IoT device / Services)
All.
Data used and data flow
1. Evidence of the personal device ecosystem behaviour that may indicate security or privacy threat are collected on the device operation. For this purpose, no sensitive data is collected. 2. Behaviour data is interpreted by CTI and self-protection components to infer threats or incidents. 3. Upon detection of an incident by the CTI, information circulates automatically in ARCADIAN-IoT to reduce the device reputation and update, as soon as possible, its authorization of communication accordingly. 4. In the case of a compromised device, the hardware will take actions to block or reduce the impact of the attack [10]. 5. In a recovery process, decentralized credentials are recovered from the blockchain component, and network credentials are recovered from the network operator. 6. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.

[10] Details removed for potential IPR protection

Main implementation risks or uncertainties
1. Personal device ecosystem behaviour monitoring and attestation, considering that a personal device has multiple services beyond the ones targeted (and are not compliant with ARCADIAN-IoT). 2. Threat detection (CTI, self-protection) and learning (federated AI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection. 4. Person identity protection combining several identification processes. 5. Automatic combination of CTI and personal device attestation with its reputation. 6. Personal device reputation models articulated with connectivity authorization enforcement. 7. Articulation of network-based authorization enforcement with hardware procedures to minimize the attack impact. 8. Decentralized credentials recovery using blockchain. 9. IoT device self-recovery process with reduced human intervention. 10. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.2. Domain B: Secured early monitoring of grid infrastructures

For demonstrating ARCADIAN-IoT framework in domain B, the following use cases were selected:

- B1: New device registration
- B2: GMS IoT device data gathering and transmission process
- B3: Service request from third-party IoT monitoring platforms
- B4: GMS IoT device security or privacy incident
- B5: GMS middleware security or privacy incident
- B6: External data audit to grid infrastructure

5.2.1 Use case B1: New device registration

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Grid infrastructure manager.
Use Case Story
This use case depicts the scenario of the service supplier configuring and registering a new IoT monitoring device that is compliant with ARCADIAN-IoT[11] to gather and propagate information from sensors and actuators of a grid infrastructure, with security and privacy, to a monitoring tool. In the grid monitoring device manufacturing, besides the firmware adapted to each grid infrastructure needs, each device is setup with a **crypto chip** and an eUICC for receiving **eSIM** profiles. In this ARCADIAN-IoT domain, the crypto chip will be the device RoT that will have personalized cryptographic information for the **hardened encryption** of the private data collected in the grid infrastructure (generated at the crypto chip or a PSK). In this case, the eSIM component will be used to provide cellular connectivity and to allow a network-based **authentication** of the device in the ARCADIAN-IoT GMS (extending current SoA, where network credentials are just used to authenticate devices in networks). The communication through the cellular network is also a key element of the domain because at the network core will live the ARCADIAN-IoT **authorization** enforcement component. This component will

[11] Definition of IoT devices compliant with ARCADIAN-IoT in D2.4

ensure that compromised devices don't communicate with services besides the ones for **recovery** from security or privacy incidents.

Moreover, an **SSI** (e.g., a **decentralized ID)** will also be generated with the device unique information (e.g. hardware-based IDs) and securely provided to it. This decentralized identifier will also be stored in ARCADIAN-IoT **blockchain** component for allowing **credentials recovery** in case of a security of data privacy incident. Therefore, ARCADIAN-IoT GMS device identification and authentication joins, at least, two factors: the well-accepted identification/authentication mechanism used in cellular networks and a decentralized approach.

After the device robust identifiers and authentication material are generated and provisioned to the device, and the device being ready for performing the hardened encryption (having the cryptographic material to encrypt the sensitive data and its firmware programmed to do so), it is registered and authenticates in the GMS middleware services. These services bootstrap the device processes of **attestation, behaviour monitoring**, **reputation** and **cyber threat intelligence** in ARCADIAN-IoT framework.

Through a compliant mobile or web interface, the GMS middleware informs the infrastructure manager[12] of the new IoT device registered for gathering and transmitting the data generated in their grid infrastructure. At this moment, the grid manager also selects (and authorizes) the device data to be forwarded to one or more specific third-party telemetry monitoring (**self-aware data privacy**). The infrastructure owner will also be informed that ARCADIAN-IoT components will monitor the device and the related third parties' behaviour to ensure his data security and privacy.

If the infrastructure owner accepts the connection of the device to the telemetry monitoring tool and to ARCADIAN-IoT framework, the GMS setup is ready to securely connect grid infrastructure sensors and actuators to one or more web/mobile monitoring tools (through the GMS IoT device and middleware). The monitoring tools themselves need to be compliant with ARCADIAN-IoT[13] to be authorized to receive the cryptographic material that decrypts the private grid data sent.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.

[12] For security purposes the grid infrastructure manager needs to comply with ARCADIAN-IoT identification procedures, having more than one robust identity mechanisms to access the GMS information.
[13] Definition of the requirements for a third-party to be compliant with ARCADIAN-IoT at D2.4

Use Case Priority
***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Operational needs and characteristics of the grid infrastructure considered in the manufacture of the IoT monitoring device (e.g. sensors and actuators secure communication with the IoT monitoring device). 2. To ensure the system security and have control over its privacy, the infrastructure owner needs to be registered in GMS services with identification and authentication mechanisms that comply with ARCADIAN-IoT. 3. (starts with the manager acceptance within this use case) ARCADIAN-IoT behaviour monitoring component oversees the interactions of the device and third-party monitoring service to, in articulation with the CTI component, trigger any security action needed and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. GMS IoT device is compliant with ARCADIAN-IoT, having a robust identity process set up, as well as the information for hardened encryption stored in the RoT. 2. Device is registered and able for being recognized by the compliant telemetry / grid infrastructure monitoring platform and start communicating data. 3. ARCADIAN-IoT behaviour monitoring and CTI components start monitoring the device behaviour in order to trigger any necessary security actions, and updating the related trust knowledge (which may include reputation and authorization changes). 4. The infrastructure owner is aware of where his data will start being sent, authorizing specific third-party monitoring tools.
Entities/Scope (Person/IoT/Apps Services)
All.
Data used and data flow
1. The network-based identifier is provisioned to the device using the eSIM GSMA-SAS standards and stored at the eUICC, which is a secure element. 2. Decentralized identifiers are generated with the device unique information (hardware IDs) and provisioned to the RoT (crypto chip) and to the blockchain component. 3. The cryptographic material for hardened encryption can be generated at the crypto chip or be a PSK provisioned by the hardened encryption component and stored at the crypto chip. 4. After, if the infrastructure manager authorizes, the device authenticates in the ARCADIAN-IoT GMS services (with both authentication factors), its behaviour starts being monitored

(behaviour monitoring component) and interpreted (CTI), its reputation and attestation are bootstrapped, and it is ready to start forwarding grid infrastructure data, encrypted to one or more monitoring tools, which needs to be compliant with ARCADIAN-IoT.
Main implementation risks or uncertainties
1. Identification and authentication certificates generation and provisioning. 2. Encryption material generation and provisioning. 3. IoT device bootstrap at ARCADIAN-IoT framework components. 4. IoT device authentication at ARCADIAN-IoT GMS and third-party monitoring tools.

5.2.2 Use case B2: Device data gathering and transmission process

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Grid infrastructure manager.
Use Case Story
At this stage, the GMS IoT device, already registered and authenticated in GMS services, starts to run its local sensors reading cycle and transmitting the payload to the monitoring service. After getting and aggregating the data from the grid infrastructure sensors the GMS IoT device performs the **hardened encryption** of the payload with RoT – crypto chip - information. Sends the encrypted payload to the GMS middleware. In the case there is no connectivity available, the device stores the encrypted data locally. When communication is back in service, the stored data is sent to GMS middleware with a timestamp assigned to the telemetry parameters (sensors data). ARCADIAN-IoT **behaviour monitoring**, **attestation,** and **CTI**, oversee and interpret the IoT device behaviour through GMS middleware, adjusting the device security and privacy **reputation** and its **authorization** to access or be accessed by online services when needed. According to the GMS monitoring rules and the infrastructure manager authorization, GMS middleware forwards the data to the compliant monitoring tools (**self-aware data privacy**). These third-party tools need to comply with ARCADIAN-IoT to be able to decrypt the GMS data[14].

[14] Definition of compliant ARCADIAN-IoT third-party services available in D2.4

If, for some reason, the device is turned off, when it is turned on again it performs the authentication in GMS services with the **network-based credentials** and the **decentralized ID** again and starts to run its local sensors reading cycle. A re-**authentication** process (authenticate again according to a condition like the time since last authentication) may be applied for security purposes.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High
Use case preconditions
1. Use case B1. 2. ARCADIAN-IoT behaviour monitoring and CTI components oversee the interactions of the IoT device and services involved to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. IoT device is transmitting encrypted data to the GMS middleware and authorized IoT monitoring tools.
Entities/Scope (Person/IoT/Apps Services)
IoT / Services.
Data used and data flow
1. The device identifiers and authentication material, cryptographic material for hardened encryption and the data gathered from the grid infrastructure (payload) are used. 2. The payload gathered from the grid sensors and aggregated for communication, and the related timestamp is encrypted with RoT information and sent to the GMS middleware. If no communication is available, it is stored encrypted in the device until the transfer is possible.

3. New authentication processes using the device identifiers, which are stored in the device secure element, are triggered if needed, according to security policies. 4. Communication events are captured by ARCADIAN-IoT framework (e.g., behaviour monitoring, CTI) to infer potential threats and act if needed.
Main implementation risks or uncertainties
1. Communication issues: data will be stored encrypted locally until communication is recovered. 2. Hardened encryption of the grid infrastructure data. 3. Authentication with multiple factors, being one stored at hardware level and other decentralized. 4. Behaviour monitoring and inference of security or privacy threats.

5.2.3 Use case B3: Service request from third-party IoT monitoring platforms

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Security; Common.
Use Case Actors
Grid infrastructure manager.
Use Case Story
Defining grid infrastructure monitoring parameterization involves sending data/commands to the IoT devices. An example can be the request to change the devices routines, e.g., change the sensor reading frequency. In this case, the grid infrastructure manager starts by authenticating in the platform with a compliant **multi-factor authentication** that uses at least one **decentralized identifier**. GMS services validate the requesting user and the app/service identity, and assess its reliability (**reputation**) to grant that person access to the services. When successfully logged in, the user selects a GMS IoT device from the grid infrastructure he has access to, and requests GMS middleware to send commands to that device. If the person and the app have the necessary **authorization**, the device data (e.g., configuration) is retrieved, encrypted, from the device, and sent to the IoT monitoring tool, which can decrypt the data sent by the device and present it to the user. The user edits the intended fields and requests the sending of the new data to the device, **encrypted** again. The updated data is kept encrypted in all the flow and only accessible (decrypted) by the GMS IoT device it is being sent to. To be able to receive the new commands, the IoT device needs to be on, connected and **securely authenticated with more than one factor** in ARCADIAN-IoT GMS middleware. When the

GMS IoT device receives the encrypted request, it **decrypts it with RoT** (crypto chip) information. If the data is successfully decrypted it means that the command was really directed to that device, and it shall be executed by its firmware. If the device cannot decrypt the request, it informs GMS middleware and discards it.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High****: critical to several project objectives and without it some objectives could not be fulfilled* ***Average****: Important, but other use cases have the same purpose* ***Low:*** *Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use case B1. 2. Grid infrastructure manager registered in the monitoring tool and with an identification compliant with an ARCADIAN-IoT person identification. 3. Third-party IoT monitoring tool (compliant with ARCADIAN-IoT) provisioned with material for decrypting/encrypting the IoT device service commands. 4. Devices RoT (crypto chips) provisioned with material for decrypting the commands sent. 5. ARCADIAN-IoT behaviour monitoring and CTI components oversees the devices and third-party service in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. If the operation is successful, GMS IoT device has new information to update its routines and updates them accordingly. 2. If the operation is not successful, the device continues with the previous routines.
Entities/Scope (Person/IoT/Apps Services)
All.

Data used and data flow
1. As data used in this use case, we have the grid infrastructure manager (person) identifiers and authentication material, third-party/monitoring tool identifiers, GMS IoT device identifiers, its current configuration and its new configuration, and cryptographic material for encrypting/decrypting the new commands. 2. Using an ARCADIAN-IoT compliant IoT monitoring tool, a user requests a specific device current configuration. Being authenticated and having the necessary authorization, the information is retrieved, decrypted at the app and editable. 3. The new commands are encrypted and sent, through the GMS middleware, to the GMS IoT device. 4. At the device, the commands are decrypted with RoT information and, if successful, applied. 5. If the device is unable to decrypt the data, informs GMS middleware and discards it.
Main implementation risks or uncertainties
1. Person / grid infrastructure manager secure authentication and trustworthy identification in GMS services through third-party IoT monitoring tool. 2. IoT device robust identification to avoid impersonation attacks. 3. Implement and enforce trustworthiness and authorization system for the participants (services, devices and person). 4. Commands encryption / decryption flow between the IoT device and the IoT monitoring tool.

5.2.4 Use case B4: GMS IoT device security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Grid infrastructure attacker(s).
Use Case Story
This use case depicts the scenario of a security or privacy incident involving a GMS IoT device. It includes the device preparation for it (for incident **detection** and **recovery**), the private data and identity **protection** and the subsequent actions of **recovery**. Examples of security or privacy incidents are the cases where the IoT device is stolen, has unauthorized access to the private data it owns/communicates, or unauthorized control or manipulation of its behaviour.

For being able to **detect, protect and recover** from a security or privacy incident, at every moment of the operational life of the GMS IoT device, information is being securely collected by ARCADIAN-IoT framework components, like the **behaviour monitoring**, and interpreted by a **cyber threat intelligence** tool. Also, for this purpose, a **federated AI** paradigm will be in place for collectively training an AI model on distributed data while ensuring **data privacy**.

For **protecting** the grid infrastructure private information, the data the device collects is kept **encrypted** and just sent to the third-party IoT monitoring tools that are compliant with ARCADIAN-IoT, authorized by the data owner (**self-aware data privacy**), and whose **reputation** indicates that are trustworthy. ARCADIAN-IoT dynamic **reputation** system defines the compliant devices and services trustworthiness according to several factors, including their **behaviour**, which is being monitored, and interpreted (**CTI**). To ensure that no unauthorized access to the grid happens, only trustworthy devices are able to receive commands that change their behaviour, and these commands can only come from trustable GMS services. Moreover, new service data for IoT devices can only be **decrypted with RoT (crypto chips) information.** The device communication capacities are kept under control with a network-based **authorization** enforcement tool, which is always aware of all devices' **reputation**.

Regarding the **IoT device identity**, to ensure its **protection**, it is composed of several factors to be used simultaneously, being at least one stored in the hardware secure element – **eSIM**/eUICC (the **network credentials**), and a second one, a **decentralized identifier**, not controlled or stored at any centralized entity. The network credentials manipulation and the **eSIM** communication with the network are done according to the GSMA security accreditation schema (GSMA-SAS).

In the case of a security **incident being detected**, the device **reputation** is updated accordingly immediately, and the accesses **authorization** enforcement as well. With this, the device can only access network services for **recovering** from the incident. Has no access to services that may provide/request private data or cryptographic material, nor has access to external services that may be controlling it, or gathering the device or grid infrastructure private data. If the device is operational, it takes actions for recovery from the incident according to the type (**self-recovery** component). Self-recovery procedures may require access to ARCADIAN-IoT services, and the **authorization** enforcement component (placed at the network provider core elements) ensures that these are the only ones available to the compromised device.

If or when the **self-recovery** processes are successful, the device software and hardware is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. Network credentials can be recovered with the network operator. The decentralized identifiers can be recovered from the ARCADIAN-IoT **blockchain** component.

Along the process, the **cyber threat intelligence** tool shares threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability. Objective 6: Self and coordinated healing with reduced human intervention. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. GMS IoT device is compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., reputation system, hardened encryption, authorization and self-recovery) are operational.
Use case postconditions
1. If the device is operational (e.g., didn't got damaged) and not stolen, the incident is mitigated, and its security and privacy is restored. 2. Threat information in the form of trained models is shared with CSIRT and CERT networks for propagating the threat awareness.
Entities/Scope (Person/IoT/Apps Services)
IoT device.
Data used and data flow
1. Evidence of the IoT device's behaviour is collected on the device operation. No sensitive data is collected, just information that allow to infer threats. 2. Periodically information to attest the device identity and integrity is also gathered. 3. Behaviour data is interpreted by CTI and Federated AI components to understand potential threats or incidents. 4. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to reduce the device reputation and update, as soon as possible, its authorization of communication accordingly. 5. In the case of a compromised device, its communication abilities will be reduced strictly to recovery processes until it is found trustworthy again. 6. In a recovery process, decentralized credentials are recovered from the blockchain component, and network credentials are recovered from the network operator. 7. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.

Main implementation risks or uncertainties
1. IoT device behaviour monitoring and integrity attestation. 2. Threat detection (CTI) and learning (federated AI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection. 4. Identity protection combining several robust identification processes. 5. Automatic combination of CTI and IoT device attestation with its reputation. 6. IoT device reputation models articulated with connectivity authorization enforcement. 7. Decentralized credentials recovery using blockchain. 8. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.2.5 Use case B5: GMS middleware security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Grid infrastructure attacker(s).
Use Case Story
This use case is the first that depicts security or privacy incidents related with a Cloud service (not a IoT device). It includes the service preparation for it (for incident **detection** and **recovery**), the private data and identity **protection** and the subsequent actions of **recovery**. Examples of security or privacy incidents are the cases of unauthorized access to private data it owns, or unauthorized control or manipulation of the service functionalities or availability (e.g., DDoS). For being able to **detect, protect and recover** from a security or privacy incident, GMS middleware service needs to be integrated with ARCADIAN-IoT components. When this happens, non-sensitive information is being securely collected by the framework components, like the **behaviour monitoring**, and interpreted by a **cyber threat intelligence** tool. Also, a **federated AI** paradigm will be in place for collectively training an AI model on distributed data while ensuring **data privacy**. For **protecting** the service private information, the service just deals with **encrypted** information, without storing cryptographic material to decrypt it. ARCADIAN-IoT dynamic **reputation** system defines the compliant service trustworthiness according to the several factors, including their **behaviour**, which is being monitored and interpreted (**CTI**). To ensure that no unauthorized accesses to the grid infrastructure happens, only services found trustworthy are able to receive and transmit commands that change the IoT devices behaviour, and these commands can only come from compliant and trusted GMS IoT monitoring tools. Moreover,

new service data for IoT devices can only be **decrypted with RoT (crypto chips) information**, therefore it is protected from compromised GMS middleware services. As soon as a service is found to be not trusted its communication capacities are kept under control with a network-based **authorization** enforcement tool, which is always aware of all services' **reputation**.

Regarding the **service identity**, to ensure its **protection**, two identification mechanisms are put in place, being one of them a **decentralized identifier** built with the service characteristics. Therefore, its identity isn't stored at any centralized computer. Furthermore, ARCADIAN-IoT **attestation** will ensure that no impersonation is possible when other agents of the IoT network use the GMS middleware services.

In the case of a security **incident being detected**, the service **reputation** is updated accordingly, and the accesses **authorization** enforcement as well. With this, the service can only access services for **recovering** from the incident. Has no access to services that may provide/request private data or cryptographic material nor has access to external services that may be controlling it, or gathering information from the grid infrastructure. If the service is operational, it takes actions for recovery from the incident according to the type (**self-recovery** component). Self-recovery procedures may require access to ARCADIAN-IoT services, and the **authorization** enforcement component (placed at the network provider core elements) ensures that these are the only ones available to the compromised service.

5. If or when the **self-recovery** processes are successful, the software is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. The decentralized identifiers can be recovered from the ARCADIAN-IoT **blockchain** component.

6. Along the process, the **CTI** tool shares threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

Objective 6: Self and coordinated healing with reduced human intervention.

Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.

Use Case Priority

***High**: critical to several project objectives and without it some objectives could not be fulfilled*

***Average**: Important, but other use cases have the same purpose*

***Low:** Nice to have, but not critical for the project objectives*

High.

Use case preconditions
1. GMS middleware service is compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., reputation system, authorization, attestations, federated AI, and self-recovery) are operational.
Use case postconditions
1. The incident is mitigated and its security and privacy are restored, with minimum human intervention. 2. Threat information in the form of trained models is shared with CSIRT and CERT networks for propagating the threat awareness.
Entities/Scope (Person/IoT/Apps Services)
Services.
Data used and data flow
1. Evidence of the GMS middleware behaviour is collected alongside its operation. No sensitive data is collected, just information that allow to infer threats. 2. Periodically information to attest the service identity is also gathered. 3. Behaviour data is interpreted by CTI and Federated AI components to understand potential threats or incidents. 4. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to reduce the service reputation and update, as soon as possible, its authorization of communication accordingly. 5. In the case of a compromised service, its communication abilities will be reduced strictly to recovery processes until it is found trustworthy again. 6. In a recovery process, decentralized credentials are recovered from the blockchain component. 7. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.
Main implementation risks or uncertainties
1. GMS middleware behaviour monitoring and attestation. 2. Threat detection (CTI) and learning (federated AI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection, with recovery ability. 4. Identity protection combining several identification processes for services. 5. Automatic combination of CTI and service attestation with its reputation. 6. Services reputation models articulated with connectivity authorization enforcement.

7. Decentralized credentials recovery using blockchain. 8. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs. 9. Processes of self-recovery from incidents with reduced human intervention.

5.2.6 Use case B6: External data audit to GMS IoT device

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Auditor and Grid infrastructure manager.
Use Case Story
This use case depicts the scenario of an authority requesting an audit to data stored locally at the GMS IoT device, after an incident. An authorized body, with the vendor of GMS technology support and an auditing tool (compliant with ARCADIAN-IoT), can access the device data for the legal/compliance purpose. Upon request from an authorized body, the GMS technology vendor provides a trustworthy auditing tool (hardware and software) that allows to retrieve the data stored in a GMS IoT device. For data protection, just specifically authorized and identified devices and services can retrieve this data. The agent from the authorized body needs to identify and authenticate himself/herself in the tool (e.g., with **eIDAs** or **VC**) in the presence of the grid infrastructure manager, who also needs to authenticate with more than one robust identification mechanism in the tool to allow the auditing process (**authentication** and **self-aware data privacy**). After the secure authentication of both persons, the agent is authorized to select the GMS IoT device and request access to its data. If the agent, the grid infrastructure manager and the auditing tool are trustworthy (according to, e.g., ARCADIAN-IoT **behaviour monitoring**, **CTI, attestation** and **reputation** components), it is granted access to the data of the selected device to the auditing tool. Data, that was **stored encrypted** at the device, is **retrieved encrypted** as well. Keys for decrypting the data are requested to ARCADIAN-IoT encryption services and, considering the entities involved trustworthiness, generated and provided to the auditing tool for the auditing purpose. These keys have time usage limit, becoming invalid after a period. The process doesn't allow any change to the integrity of the data in the device, just to analyse the data stored. After the auditing process, with the agent logout in the tool, all the data and related cryptographic material is deleted from it.

Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
Average.
Use case preconditions
1. Use case B1. 2. Auditor and grid infrastructure manager have identification credentials compliant with ARCADIAN-IoT persons identification, being at least one a decentralized approach (SSI, DID, VC). 3. Auditing tool is compliant with ARCADIAN-IoT (being therefore integrated with the framework components and known by the system – previously registered). 4. Audited GMS IoT device had an incident that demands auditing. 5. ARCADIAN-IoT framework components (e.g., behaviour monitoring, attestation, reputation system, authorization, and self-recovery) are operational.
Use case postconditions
1. Auditing process finished. 2. Data from the auditing process deleted from auditing tool. 3. GMS IoT device should go through an incident recovery process before being placed back in an operational scenario.
Entities/Scope (Person/IoT/Apps Services)
All.
Data used and data flow
1. Data for identification and authentication of the auditor, of the grid infrastructure manager and of the auditing tool is sent to the ARCADIAN-IoT framework authentication component. If the persons, the device and the software it runs are found trustworthy according to the reputation system the auditor is able to authenticate in GMS with the auditing tool.

2. The auditor selects the device target of auditing and requests its data. Authorization to access the device data needs to be given by the grid infrastructure manager. 3. If authorization is provided, the data that is stored encrypted in the device is retrieved to the auditing tool. 4. ARCADIAN-IoT encryption component generates keys for decryption of the data for auditing purposes, granting them to the specific auditing tool. 5. The auditing tool, with the authorized auditor authenticated, decrypts the data, and makes it visible to him/her. Data is read-only. 6. At the end of the process, when one of the actors logs out from the auditing tool, all the data and cryptographic material is automatically deleted from the auditing tool.
Main implementation risks or uncertainties
1. Auditor (person external to the business) identification with eIDAs, VC or other robust identification mechanism and authenticated in ARCADIAN-IoT using the auditing tool. 2. Two authorized persons simultaneous authentication with robust identification mechanisms to access auditing data. 3. Secure auditing tool for grid infrastructure IoT devices integrated with ARCADIAN-IoT components. 4. Secure encryption/decryption flow for audit purposes.

5.3. Domain C: Medical IoT

For demonstrating ARCADIAN-IoT in domain C, the following use cases were selected:

- C1: MIoT kit delivery - Patient registration and authentication
- C2: MIoT capturing and sending vital signs and perceived health status
- C3: Personal data processing towards health alarm triggering
- C4: Monitoring a patient and updates to the patient monitoring protocol
- C5: Patient MIoT devices security or privacy incident
- C6: MIoT services security or privacy incident
- C7: Medical third-party security or privacy incident

5.3.1 Use case C1: MIoT kit delivery - Patient registration and authentication

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Patient and Medical professional.
Use Case Story
This use case depicts the scenario of the enrolment of a new patient to be monitored at home with the compliant ARCADIAN-IoT medical solution. It starts at the hospital (e.g., in the Oncology Services), when the medical IoT (MIoT) kit is assigned to the patient. The MIoT kit includes a smartphone with a specific mobile app installed and a set of medical sensors that communicate with the hospital monitoring system through the provided smartphone (sensors are already paired and synced with the smartphone). An authorized medical professional (doctor, nurse or other) requests the patient to register himself/herself using the MIoT app, in a smartphone that is going to be assigned to him/her. At this stage the device is completely free of any personal data of previous patients. When the person opens the MIoT app is presented with information from ARCADIAN-IoT framework referring that the **service is compliant** with its data security and privacy procedures[15]. This means that, for example, the security behaviour of that device, of the MIoT app and of all the MIoT services are continuously monitored (**behaviour** and **flow monitoring**) and interpreted **(CTI** and **self-protection components)** and have an associated and up-to-date

[15] Definition of the requirements for being an ARCADIAN-IoT compliant third-party is presented at D2.4

trustworthiness **reputation**. The security reputation of the MIoT entities involved is presented to the patient at this moment.

Willing to proceed, the person is informed in the app that a **personal RoT**, in this case a unique **eSIM**, will be generated for him/her and provisioned to the smartphone.

With the patient authorization, having the RoT in the device, cryptographic material for encryption/decryption of his/her personal health data is generated and sent securely to the device RoT. Alternatively, the cryptographic material is generated in the mobile device RoT itself. This cryptographic material, stored in the device RoT, is used in the **hardened encryption** of the health data gathered, before being sent to the network.

After having the personal RoT prepared for the hardened encryption process, the patient proceeds with the registration procedure, filling a form with the personal data needed for the MIoT services, part of which is used for generating his/her **self-sovereign identity (SSI)** (e.g., **decentralized identifiers** or **verifiable credentials** - non-centralized credentials that will allow to identify and authenticate him/her in the MIoT services). The data provided by the person and the smartphone identification is encrypted with RoT information and submitted to the MIoT services. The patient is informed that identifiers for secure and private identification are going to be generated based on the data provided. The generated identification credentials are backed up in a **permissioned blockchain** for the case of the need for **recovery** of a lost/stolen identity.

After the generation of the SSI, the MIoT services request to store the credentials securely at the device RoT. Alternatively, it can be stored in a secure ID wallet. When the person authorizes, ARCADIAN-IoT securely provisions and stores the identification and authentication material in the personal device (RoT or ID wallet).

The patient is informed that his/her new network credentials, associated with the **eSIM/RoT**, are unique and will be used as a **second secure zero-touch identification/authentication mechanism** of the person and device in the MIoT services.

For closing the registration of the patient in the smartphone, ARCADIAN-IoT **attestation** component collects and stores the necessary information for future assessment of changes that may imply a security/privacy breach. Afterwards, the person is informed in the app that the registration procedure will be finished by the medical staff.

At this stage, the medical professional, securely authenticated in the MIoT Monitoring solution, can see that the patient is correctly enrolled in the system and the device it used for the enrolment, and just confirms the delivery of the equipment to that person. Any explanation regarding the use of the equipment is done at this stage, including that the patient will be informed, in the MIoT app, when a doctor requests to monitor the health data. The patient needs to accept the doctor to see his/her health data. The same happens for the MIoT data processing module that generates health alarms (the patient needs to authorize it). For patients with low technological literacy this can be explained by the medical professional personally and the authorization to the person's doctor and to the generation of alarms granted at that moment. The patient is now registered and has the equipment configured to start being used in his/her home.

At home, for authentication, the MIoT app requests authorization to retrieve and use the user **decentralized identifiers / verifiable credentials / network credentials** (about the person and the personal device) from the RoT or wallet ID. For accessing the app itself, a biometric factor may apply (e.g., fingerprint and/or pin).

If permission is given, **identification and authentication** data is retrieved and used to login the user in the MIoT services with more than one simultaneous factor. The app itself also presents its identification to the services.

If the user, the smartphone and the app are authorized to access MIoT services (are compliant with ARCADIAN-IoT and, according to the **reputation** model, are trustable), the login process is successful and the MIoT app is securely informed that the monitoring protocol can proceed.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. MIoT services and app are compliant with ARCADIAN-IoT. 2. Smartphone provided in the MIoT kit has eUICC. 3. Medical staff is registered in MIoT monitoring services with authentication and identification compliant with ARCADIAN-IoT. 4. Health sensors are securely paired with the smartphone (ARCADIAN-IoT components act in the smartphone for securing the person and health devices trust, security and privacy management).
Use case postconditions
1. Patient registration and authentication done. Can start using the MIoT kit at home. 2. ARCADIAN-IoT behaviour monitoring and CTI components start overseeing the device behaviour in order to trigger any necessary security actions, and updating the related trust knowledge (which may include reputation and authorization changes). 3. The patient can be made aware of where his/her data will start being sent, authorizing since this moment specific doctors.
Entities/Scope (Person/IoT/Apps Services)
All.

Data used and data flow
1. Patient data, to be defined in the research process, flows encrypted from the smartphone (MIoT app) to ARCADIAN-IoT services. In these services, an SSI is generated and placed in a permissioned blockchain for restoring in case of need. The necessary personal identification data is returned to the user and stored in a secure ID wallet or in the RoT. 2. Information for hardened encryption is provided to or generated at the user mobile device (stored securely in the RoT). Information for decrypting user data is securely sent to ARCADIAN-IoT third-party services, when needed, if these have a trustworthy reputation. The person needs authorize the services to access his/her data. 3. At the authentication step, the ARCADIAN-IoT compliant app requests the authentication data from the RoT and/or an ID wallet. If the app is trustable and access is given, data is retrieved from the secure element to the device and the flow continues from the MIoT smartphone to MIoT services. In these services, the ARCADIAN-IoT authentication process happens with more than one authentication factor and, if successful, information about that is securely returned to the device authorizing the patient to proceed (start the health monitoring). 4. The medical professional views the new patient registration in the monitoring tool and accepts it. The patient may authorize at this moment his doctor to access his/her health data. Only authorized doctors can access each patient data.
Main implementation risks or uncertainties
1. Person and device identification and authentication certificates generation and provisioning. 2. Encryption material generation and provisioning. 3. Implement a trust model based on reputation that allows the patients to know the services trustworthiness. 4. MIoT smartphone bootstrap at ARCADIAN-IoT framework components. 5. MIoT patient and app authentication at ARCADIAN-IoT MIoT services and third-party monitoring tools. 6. Patient authorization to specific doctors (who need to have an identification compliant with ARCADIAN-IoT as well).

5.3.2 Use case C2: MIoT capturing and sending vital signs and perceived health status

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Patient.

Use Case Story
At this stage, the patient is at home with the sensors placed in the body and synced with the smartphone. The MIoT app, authenticated in MIoT services, starts to run the health sensors reading cycle. When needed or according to the health monitoring plan, the patient also provides the perceived health status in the app. After getting and aggregating the data from the health sensors, the app in the smartphone, which works like a gateway between the sensors and the MIoT services, performs the **hardened encryption** of the payload with RoT – **eSIM** - information. The same happens if the patient uses the app form to inform about his/her perceived health status. The information is encrypted with RoT information in the smartphone before being sent. The smartphone sends the encrypted payload to the MIoT middleware services. In the case there is no connectivity available, the device stores the **encrypted** data locally. When communication is back in service, the stored data is sent to MIoT services with a timestamp assigned to the sensors data / perceived health status. With the patient authorization, MIoT middleware forwards the data to the compliant hospital monitoring tools. These third-party tools need to comply with ARCADIAN-IoT[16] to be able to decrypt the MIoT data. Decryption only happens with the patient authorization to a specific medical professional (which can be given in the hospital – C1) – **self-aware data privacy**. If, for some reason, the smartphone is turned off, when it is turned on again it requests the patient to do the authentication in MIoT services with the **network-based credentials** (stored at hardware level) and the **SSI** (decentralized) again and starts to run the health sensors reading procedure. A biometric identification to access the app can apply as well (can be configured in the hospital when the smartphone is given to the person). A re-**authentication** process (authenticate again according to a condition like the time since last authentication) may be applied for security purposes.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.

[16] Requirements for a third-party to be compliant with ARCADIAN-IoT in D2.4

Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use case C1. 2. Sensors are well placed (app can help by informing when data is not being well received). 3. ARCADIAN-IoT behaviour monitoring and CTI components oversee the interactions of the IoT device (the IoT gateway) and services involved in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the parties involved.
Use case postconditions
1. MIoT app is transmitting encrypted data to the MIoT middleware, which can be forwarded, encrypted as well, to authorized IoT monitoring tools.
Entities/Scope (Person/IoT/Apps Services)
All.
Data used and data flow
1. The data used in this use case are user identifiers and authentication material (from device, app and person), cryptographic material for hardened encryption and the data gathered from the health sensors (payload). 2. The payload gathered from the health sensors and aggregated for communication, and the related timestamp, are encrypted with RoT information and sent to the MIoT middleware. If no communication is available, the payload is stored encrypted in the device until the transfer is possible. 3. New authentication processes using the device identifiers, which are stored in the device secure element and/or are decentralized, are triggered if needed, according to security policies. 4. Communication events are captured by ARCADIAN-IoT framework (e.g., behaviour monitoring, CTI) to infer potential threats and act if needed.
Main implementation risks or uncertainties
1. Communication issues: data will be stored encrypted locally until communication is recovered. 2. Hardened encryption of the health data with RoT information. 3. Behaviour monitoring and inference of security or privacy threats. 4. Robust identification and authentication according to security policies.

5. Implementation of authorization policies to access the patients' data in the hospital, ensuring privacy self-awareness.

5.3.3 Use case C3: Personal data processing towards health alarm triggering

ARCADIAN-IoT Layers
Vertical plane: Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Patient.
Use Case Story
This use case refers to the health data processing, in the cloud (in a data processing unit of MIoT middleware), with the purpose of detecting and triggering health alarm conditions in the hospital monitoring tool. Having the data that results from C2, which comes encrypted from the patient MIoT smartphone, for being able to detect any alarm condition, the data needs to be decrypted. Furthermore, it will likely need to exist decrypted in a centralized system to allow building intelligent models that trigger alarm conditions based on variations of health data for a particular subject. This MIoT processing unit needs to be compliant with ARCADIAN-IoT and the patient needs to authorize the processing of his/her data for this purpose (**self-aware data privacy**). If / when that happens cryptographic material to decrypt the data is provided to this module. If the patient revokes the grant for processing his/her data, new cryptographic material for encrypting/decrypting the data is generated and distributed, not being provided to this unit. To ensure the patient privacy and keep him/her anonymous in the processing unit of MIoT services, the decryption techniques applied will just decrypt the payload (sensor data), keeping the **person identity encrypted/anonymized** at all times. If needed, the payload that the processing unit receives should include aspects like age or gender, and pathological data, to be able to infer the alarm conditions without identifying the individual. ARCADIAN-IoT **behaviour monitoring**, and **CTI**, oversee and interpret this MIoT service behaviour, adjusting its trustworthiness **reputation** and its **authorization** to continue receiving health data from patients, which is revoked if the service is found not to be trusted. According to medical protocols or related health patterns learned from other patients (all anonymous) the MIoT processing unit detects alarm conditions. When detected, these alarm conditions are encrypted and merged with the encrypted identification of the patient. With the patient authorization, MIoT middleware forwards the encrypted data that includes the alarms to the compliant hospital monitoring tools. To be able to decrypt the alarms, these third-party tools need, as all that comply with ARCADIAN-IoT, to have robust identity and authentication mechanisms, allow security behaviour monitoring and need to authenticate in ARCADIAN-IoT MIoT services to receive the cryptographic material to decrypt the data sent

to them. Decryption, by the medical staff, only happens with the patient authorization (which can be given in the hospital – C1).
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High
Use case preconditions
1. Use case C2 2. ARCADIAN-IoT behaviour monitoring and CTI components oversees the interactions of the services involved in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the service.
Use case postconditions
1. When relevant, patient health alarms are triggered and sent to the hospital encrypted
Entities/Scope (Person/IoT/Apps Services)
Services
Data used and data flow
1. Patient identification and health data are used in this use case. 2. When arriving the MIoT middleware, coming from MIoT kit (health sensors and gateway), the part of the health data is decrypted, keeping the patient identification encrypted (the service does not have authorization to decrypt patient identification). 3. The health data is kept in a time series associated with that patient (who is anonymous to the system) and processed according to health rules to infer alarm conditions.

4. If an alarm condition is detected, it is encrypted and sent to the monitoring tool to be seen by authorized medical staff.
Main implementation risks or uncertainties
1. Securely process patients' data, keeping the person privacy ensured and under his/her control. 2. Monitor the processing unit behaviour and infer threats/vulnerabilities that can endanger private data.

5.3.4 Use case C4: Monitor a patient and update the patient monitoring protocol

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Medical professional.
Use Case Story
Even though it depends on the data collected in the medical IoT devices, monitoring patients is one of the most relevant functional use cases of the whole medical IoT domain. The system is thought to monitor patients in an efficient and secure way, while they are at home. Related to the patient monitoring, which can lead to decisions to change medical protocols, is the sending data/commands to the medical IoT devices. An example can be the request to change the devices reading frequency, or just request the patient to say how he/she feels more often (through the app). In this case, a medical professional authenticates in the MIoT hospital platform with a **strong multi-factor authentication**, where one of the factors is an **SSI**. MIoT services validate the requesting user and the app (MIoT hospital platform) identity and assess its reliability (**reputation**) to grant him/her access to the services. When successfully logged in, the medical professional selects a patient to whom he/she has access to, or requests access to a new patient. The medical professional can also have a dashboard for monitoring several patients that authorized the access to their data to that professional, and this dashboard can include a section with health alerts related with those patients. Patient's data is kept encrypted until being requested by an authorized medical professional. At this moment it is decrypted with cryptographic material provided by ARCADIAN-IoT **self-aware data privacy** and **hardened encryption** to the third-party tool (MIoT hospital platform) if it is, according to the **reputation** system, trustworthy. If the medical professional wants to change the monitoring protocol of a given patient, it requests MIoT services to send commands to that patient MIoT app.

If the medical professional and the services he/she is using have the necessary **authorization**, the MIoT app configuration data is retrieved, encrypted, from the smartphone, and sent to the MIoT hospital platform. Having the necessary authorization, the MIoT hospital platform decrypts the data sent by the patient app and presents it to the medical professional. The user edits the intended fields and requests the sending of the new data to the MIoT app, **encrypted** again. The updated data is kept encrypted in all the flow and only accessible (decrypted) by the MIoT app, in the device (smartphone) it is being sent to. To be able to receive the new commands, the smartphone needs to be on, connected and the patient **securely authenticated with more than one factor** in ARCADIAN-IoT MIoT middleware. When the patient device and the MIoT app receive the encrypted request, it **decrypts it with RoT** (eSIM) information. If the data is successfully decrypted it means that the command was really directed to that device, and it shall be executed by the app. If the device cannot decrypt the request, it informs MIoT middleware and discards it.
Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. Objective 2: Enable security and trust in the management of objects' identification. Objective 3: Enable distributed security and trust in management of persons' identification. Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Use case C1. 2. Medical professional, user of the MIoT hospital platform registered and with an identification compliant with an ARCADIAN-IoT person identification. 3. Medical professional authorized by a patient (or more) to decrypt his health data for well-being monitoring purposes. 4. MIoT hospital platform provisioned with material for encrypting the commands sent. 5. Devices RoT (eSIM) provisioned with material for decrypting the commands sent.

6. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the entities involved in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include dynamic reputation and authorization changes for the service.
Use case postconditions
1. Authorized medical staff is able to monitor a patient health and update the medical protocol. 2. In the case of a medical protocol change, the MIoT kit has new information to update the medical monitoring routines.
Entities/Scope (Person/IoT/Apps Services)
All.
Data used and data flow
1. The data used in this use case includes the medical professional identifiers and authentication material, third-party/monitoring tool identifiers, patient identifiers, his/her medical data, generated alarms, and cryptographic material for decrypting the person health data in the monitoring tool. The current medical monitoring protocol and a new one may be used as well, and the related cryptographic material for encrypting/decrypting the new protocol. 2. Regarding the patient health monitoring in the hospital MIoT tool, a medical professional, after being authenticated (according to the ARCADIAN-IoT compliance protocol described in D2.4), requests the access to a patient data record. If he/she is authorized (trustworthy) to access patients' data, and if that patient has authorized that medical professional to access his/her data, and the service he/she is using is trustworthy, the data is retrieved and decrypted. Data includes the health readings (shown in a relevant format) and health alarms. After the professional logs out from the system, the patient decrypted data and related cryptographic material is deleted. 3. Also, in the MIoT monitoring tool, for changing a given patient medical protocol, the same authorized professional with access to that patient data, requests the change. Being authenticated and having the necessary authorization, the information is retrieved encrypted from the patient device. It is decrypted in the platform and editable for the medical professional to change it. The new commands are encrypted and sent, through the MIoT middleware, to the patient device. At the device, the commands are decrypted with RoT information and, if successful, applied. If the device is unable to decrypt the data, informs MIoT middleware and discards it. ARCADIAN-IoT components monitor the event and acts accordingly.
Main implementation risks or uncertainties
1. Medical staff robust identification and authentication in the third-party monitoring tool (which needs to be compliant with ARCADIAN-IoT). 2. Securely granting access to authorized medical staff to patient health records, collected with the MIoT kit, and to the processed health alarms, with the person self-awareness of his/her data privacy (i.e., who accesses what and when). 3. Securely change the medical protocol in the MIoT kit using the compliant third-party tool.

5.3.5 Use case C5: Patient MIoT devices security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Attacker(s).
Use Case Story
This use case depicts the scenario of a security or privacy incident involving the patient MIoT devices (smartphone/app and sensors). Although we start by purposely referring the health sensors, given that the smartphone/app is the gateway for the sensors' communication with the internet, our actions will focus on protecting the patient data collected at the sensors in the smartphone[17]. It includes the device preparation for it (for incident **detection** and **recovery**), the private data and identity **protection** and the subsequent actions of **recovery**. Examples of security or privacy incidents are the cases where the smartphone is stolen, or hacked (e.g., unauthorized access to private data it owns, or unauthorized control or manipulation of the device/app behaviour). For being able to **detect, protect and recover** from a security or privacy incident, at every moment of the operational life of the patient MIoT devices, (non-personal) information is being securely collected by ARCADIAN-IoT framework components, like the **behaviour monitoring**, **flow monitoring** and interpreted by a **CTI** tool. Also, for this purpose and supporting these components action, a **federated AI** paradigm will be in place for collectively training an AI model on distributed data while ensuring **data privacy**. Moreover, a **self-protection** component will also be in place inferring threats based on the data received from, e.g., the flow monitoring, and on intent-based protection rules. This component dynamically decides which rules to apply to protect MIoT devices and the IoT network (e.g., from DDoS attacks). For **protecting** the patient private information, the data the smartphone collects with the compliant app is **encrypted** and kept that way. It is just sent to medical third parties that are compliant with ARCADIAN-IoT, authorized by the patient (**self-aware data privacy**), and whose **reputation** indicate that are trustworthy. ARCADIAN-IoT dynamic **reputation** system defines the compliant persons, devices and services trustworthiness according to several factors, including their **behaviour**, which is being monitored and interpreted (**CTI**). To ensure that no unauthorized control of the sensors happen, only trustworthy smartphones/apps are able to receive commands that change their behaviour, and these commands can only come from trustable MIoT services. Moreover, new service data for health sensors can only be **decrypted with RoT (eSIM) information**, and a hardware-based procedure to minimize the impact of attacks will be put in place[18]. Moreover, the device communication capacities are kept under

[17] Attacks specifically to the health sensors are not considered because the risk for capturing identifiable personal data is low (sensors just collect discrete values with no identification)
[18] Details removed for potential IPR protection

control with a network-based **authorization** enforcement tool, which is always aware of all devices' **reputation**.

Regarding the **patient identity**, to ensure its **protection**, it is composed of several factors to be used simultaneously, being at least one stored in the hardware secure element – **eSIM**/eUICC (the **network credentials**) - and a second one, a **SSI**, not controlled or stored at any centralized entity in the Cloud (stored securely in the secure element of the RoT or at an ID wallet). The network credentials manipulation and the **eSIM** communication with the network follow the GSMA security accreditation schema.

In the case of a security **incident being detected**, the smartphone/person/app trustworthiness **reputation** is updated accordingly, and the accesses **authorization** enforcement as well. With this, the MIoT app can only access network services for **recovering** from the incident. Has no access to services that may provide/request private data or cryptographic material. If the device/app is operational, it takes actions for recovery from the incident according to the type (**self-recovery** and **self-healing** components). Self-recovery and self-healing procedures may require access to ARCADIAN-IoT services, and the dynamic **authorization** enforcement component (placed at the network provider core elements) ensures that these are the only ones available to the compromised device until it recovers from the incident. The self-recovery component focuses on the recovery of the data and the self-healing focuses on the recovery of the system functionalities.

If or when the **self-recovery** and **self-healing** processes are successful, the device software and hardware are restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. Network credentials can be recovered with the network operator. The **SSI** can be recovered from the ARCADIAN-IoT **blockchain** component. The human intervention is reduced to the strictly necessary in healing and recovery procedures.

Along the process, the **cyber threat intelligence** tool shares threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

Objective 6: Self and coordinated healing with reduced human intervention.

Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.

Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. MIoT devices are compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., reputation system, authorization, self-protection, self-recovery) are operational.
Use case postconditions
1. If the device is operational (e.g., is not damaged) and not stolen, the incident is mitigated and its security and privacy is restored with reduced human intervention. 2. Threat information in the form of trained models is shared with CSIRT and CERT.
Entities/Scope (Person/IoT/Apps Services)
Person and IoT device.
Data used and data flow
1. Evidence of the MIoT device ecosystem behaviour that may indicate security or privacy threat is collected on the device operation. For this purpose, no sensitive data is collected. 2. Behaviour data is interpreted by CTI and self-protection components to infer threats or incidents. 3. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to decrease the MIoT device trustworthiness reputation and update, as soon as possible, its authorization of communication accordingly. 4. In the case of a compromised device, a hardware procedure will be put in place to reduce the action of that device[19]. 5. In a recovery process, decentralized credentials are recovered from the blockchain component, and network credentials are recovered from the network operator. 6. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.

[19] Details removed for potential IPR protection

Main implementation risks or uncertainties
1. IoT device behaviour, flow monitoring, and attestation. 2. Threat detection (CTI, self-protection) and learning (federated AI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection. 4. Identity protection combining several identification processes. 5. Automatic combination of CTI and IoT device attestation with its reputation. 6. IoT device reputation models articulated with connectivity authorization enforcement. 7. Decentralized credentials recovery using blockchain. 8. IoT device self-recovery and self-healing with reduced human intervention. 9. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.3.6 Use case C6: MIoT Cloud services security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Attacker(s).
Use Case Story
This use case depicts security or privacy incidents related with a MIoT Cloud services (e.g., the data processing module for health alarm triggering). It includes the services preparation for it (for incident **detection** and **recovery**), the private data and identity **protection** and the subsequent actions of **recovery** and **healing**. Examples of security or privacy incidents are the cases of unauthorized access to private data the Cloud service owns, or unauthorized control or manipulation of the service functionalities (e.g., with DDoS attack). For being able to **detect, protect and recover** from a security or privacy incident, each MIoT Cloud service needs to be integrated with ARCADIAN-IoT components. When this happens, information is being securely collected by the framework components, like the **behaviour monitoring** and **flow monitoring** and interpreted by a **cyber threat intelligence** tool. A **self-protection** component will also be in place inferring threats based on the data received from, e.g., the flow monitoring, and based on intent-based protection rules. This component dynamically decides which rules to apply to protect the services (e.g., from DDoS attacks) Some MIoT services need to decrypt patients' private data (e.g., the service for intelligent health alarms triggering). For **protecting** the patients' private information, the service is just able to

decrypt the part of the payloads that has the health data. Apart from that, the service just deals with **anonymized** patient identity, not even having access to cryptographic material to decrypt it. The MIoT services that don't need decrypted patient data just have access to **encrypted** payloads.

Also for protection and for triggering incident mitigation measures, ARCADIAN-IoT dynamic **reputation** system defines the compliant services trustworthiness according to the several factors, including their **behaviour** and **data flow**, which is being monitored and interpreted (**CTI** and **self-protection**).

Regarding each **service identity**, to ensure its **protection**, there is a **decentralized identifier** built with the service characteristics. Therefore, its identity is not stored at any centralized computer. Furthermore, ARCADIAN-IoT **attestation** will attempt to assure that no impersonation is possible when other agents use the MIoT services.

In the case of a security **incident being detected**, the service **reputation** is updated accordingly immediately, and the accesses **authorization** enforcement as well. With this, the service can only access network services for **recovering** from the incident. Has no access to services that may provide/request private data or cryptographic material. If the service is operational, it takes actions for recovery from the incident according to the type (**self-recovery** and **self-healing** components). The self-recovery component focuses on the recovery of the data and the self-healing focuses on the recovery of the system functionalities.

If or when the **self-recovery** and **self-healing** processes are successful, the software is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. The decentralized identifiers can be recovered from the ARCADIAN-IoT **blockchain** component. The human intervention is reduced to the strictly necessary in healing and recovery procedures.

For protecting the **business continuity** of the MIoT services, the **self-healing** component will incorporate a decision manager and a resource inventory (devices and topological information of the Cloud network) to know where to heal the network, how to heal and from what to heal, being this process performed without any human intervention.

Along the process, the **cyber threat intelligence** tool shares relevant threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust.

Objective 5: Provide a hardened encryption with recovery ability.

Objective 6: Self and coordinated healing with reduced human intervention.

Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.

Use Case Priority
***High**: critical to several project objectives and without it some objectives could not be fulfilled*
***Average**: Important, but other use cases have the same purpose*
***Low:** Nice to have, but not critical for the project objectives*
High
Use case preconditions
1. MIoT Cloud services are compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., behaviour monitoring, flow monitoring, reputation system, authorization, self-protection, self-recovery) are operational.
Use case postconditions
1. The incident is mitigated and its security and privacy are restored, with minimum or none human intervention. 2. Threat information in the form of trained models is shared with CSIRT and CERT.
Entities/Scope (Person/IoT/Apps Services)
Services.
Data used and data flow
1. Evidence of the MIoT service behaviour and data flow is collected alongside its operation. No sensitive data is collected, just information that allow to infer threats. 2. Periodically information to attest the service identity is also gathered. 3. Behaviour and flow data is interpreted by CTI and self-protection components to understand potential threats or incidents. 4. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to reduce the service reputation and update, as soon as possible, its authorization of communication accordingly. 5. In the case of a compromised service, its communication abilities will be reduced strictly to recovery processes until it is found trustworthy again. 6. The recovery process, encompasses credentials recovery, where decentralized credentials are recovered from the blockchain component; data recovery, from the self-recovery component; and functionalities recovery, with the self-healing component. 7. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.

Main implementation risks or uncertainties
1. MIoT service behaviour, flow monitoring, and attestation. 2. Threat detection (CTI). 3. Novel multi-party data encryption/decryption processes for sensitive data protection, with separation of the person's identity from their data when relevant. Identity protection concerning health data. 4. Automatic combination of CTI, self-protection and service attestation with its reputation. 6. IoT services reputation models articulated with connectivity authorization enforcement. 7. Decentralized credentials recovery using blockchain. 8. IoT service self-recovery and self-healing with reduced human intervention. 9. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.3.7 Use case C7: Medical third-party security or privacy incident

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Attacker(s).
Use Case Story
This use case depicts security or privacy incidents related with the medical third-party service, which receives patients' data for health monitoring. It includes the services preparation for incident **detection** and **recovery**, the patient and medical staff private data and identity **protection** actions, and the subsequent measures of **recovery** of data and **healing** of functionalities. Examples of security or privacy incidents are the cases of unauthorized access to private patient data, or unauthorized control or manipulation of the service functionalities (e.g., DDoS). As for all the services compliant with ARCADIAN-IoT, to be able to **detect, protect and recover** from a security or privacy incident, each third-party medical service needs to be integrated with ARCADIAN-IoT components. When this happens, information is being securely collected by the framework components, like the service **behaviour monitoring** and **flow monitoring,** and interpreted by a **cyber threat intelligence** tool.

The hospital monitoring services need to decrypt patients' private data. To **protect** the patients' private information, data is kept **encrypted** until an authorized and trustworthy professional requests access to it, dully authenticated in the system. At this moment, decryption material is requested to ARCADIAN-IoT services and, if all the entities involved are found trustworthy, data is decrypted and shown in the form of dashboards with patient health variables, or patient health alerts. Upon the professional logout from the medical system, plain data used for the monitoring services is deleted, keeping just the encrypted version with no keys to decrypt it.

Also for protection and for triggering **incident mitigation measures**, ARCADIAN-IoT dynamic **reputation** system defines the compliant medical services trustworthiness according to several factors, including their **behaviour** and **data flow**, which is being monitored and interpreted (**CTI** and **self-protection**).

Regarding each **service identity**, to ensure its **protection**, it is a **decentralized identifier** built with the service characteristics and built-in in its calls. Therefore, its complete identity is not stored at any centralized computer. Furthermore, ARCADIAN-IoT **attestation** will ensure that no impersonation is possible to request patients' data or decryption material from MIoT services.

In the case of a security **incident being detected**, the service **reputation** is updated accordingly immediately, and the accesses **authorization** enforcement as well. With this, the service can only access network services for **recovering** from the incident. Has no access to services that may provide/request private data or cryptographic material. If the service is operational, it takes actions for recovery from the incident according to the type (**self-recovery** and **self-healing** components). The self-recovery component focuses on the recovery of the data and the self-healing focuses on the recovery of the system functionalities.

If or when the **self-recovery** and **self-healing** processes are successful, the software is restored to a status of compliance with ARCADIAN-IoT, which includes the **credentials recovery**. The decentralized identifiers can be recovered from the ARCADIAN-IoT **blockchain** component. The human intervention is reduced to the strictly necessary in healing and recovery procedures.

For protecting the **business continuity** of the MIoT services, the **self-healing** component will incorporate a decision manager and a resource inventory (devices and topological information of the Cloud network) to know where to heal the network, how to heal and from what to heal, being this process performed without any human intervention.

Along the process, the **cyber threat intelligence** tool shares relevant threat information in the form of trained models (not the actual data) with CSIRT and CERT networks for propagating the threat awareness.

Relation with ARCADIAN-IoT Objectives

Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework.

Objective 2: Enable security and trust in the management of objects' identification.

Objective 3: Enable distributed security and trust in management of persons' identification.

Objective 4: Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust. Objective 5: Provide a hardened encryption with recovery ability. Objective 6: Self and coordinated healing with reduced human intervention. Objective 7: Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory.
Use Case Priority ***High**: critical to several project objectives and without it some objectives could not be fulfilled* ***Average**: Important, but other use cases have the same purpose* ***Low:** Nice to have, but not critical for the project objectives*
High.
Use case preconditions
1. Medical third-party platform is compliant with ARCADIAN-IoT (being therefore integrated with the framework components). 2. Related ARCADIAN-IoT framework components (e.g., behaviour monitoring, flow monitoring, reputation system, authorization, self-protection, self-recovery) are operational.
Use case postconditions
1. The incident is mitigated and its security and privacy are restored, with minimum or none human intervention. 2. Threat information in the form of trained models (not the actual data) is shared with CSIRT and CERT.
Entities/Scope (Person/IoT/Apps Services)
Services and person.
Data used and data flow
1. Evidence of the medical third-party service behaviour and data flow is collected alongside its operation. No sensitive data is collected, just information that allow to infer threats. 2. Periodically information to attest the service identity is also gathered. 3. Behaviour and flow data is interpreted by CTI and self-protection components to understand potential threats or incidents. 4. Upon detection of an incident, information circulates automatically in ARCADIAN-IoT to reduce the service reputation and update, as soon as possible, its authorization of communication accordingly. 5. In the case of a compromised service, its communication abilities with the platform will be reduced strictly to recovery processes until it is found trustworthy again. The recovery process, encompasses credentials recovery, where decentralized credentials are recovered from

the blockchain component; data recovery, from the self-recovery component; and functionalities recovery, with the self-healing component. 6. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.
Main implementation risks or uncertainties
1. Medical third-party service behaviour, flow monitoring, and attestation. 2. Threat detection (CTI) and self-protection. 3. Novel multi-party data encryption/decryption processes for sensitive data protection, with real-time operations synchronized with the medical staff log in and log out. 4. Automatic combination of CTI, self-protection and service attestation with its reputation. 5. IoT services reputation models. 6. Decentralized credentials recovery using blockchain. 7. IoT service self-recovery and self-healing with reduced human intervention. 8. Threat sharing models for dissemination of knowledge to CSIRTs and CERTs.

5.4. Use cases verification and validation

As described in section *3. Research Methodology*, the final step on the use cases specification focused on perfecting the existent set towards meaningfulness, completeness, and coherence. Just use cases that are relevant for the validation of the project objectives were kept, ensuring as well that all the project objectives could be validated with the existent set. Despite this final stage goals, the process of verification and validation of the use cases was part of the iterative process of specification. In fact, as can be seen in Figure 2, the research process had a step of *assessment* in each iteration, that had the purpose of analysing the existent set of use cases towards its improvement.

The verification and validation of the set of use cases can be done by answering two questions:

1. Are all the project objectives considered in the use cases specified?
2. Are we able to measure all the project KPIs with the implementation of the specified usage scenarios?

Regarding question 1, as can be seen in the use cases specification, in the field *Relation with ARCADIAN-IoT objectives* are represented all the 7 objectives of the project (more than once).

Domain A: Emergency and vigilance using drones and IoT			Use Cases							
			A1	A2	A3	A4	A5	A6	A7	
			Person registration at DGA service	Person authentication at the DGA service	Person retrieving and editing personal data	Person requesting a DGA service	DGA service	Drone security or privacy incident	Personal device security or privacy incident	*Number of component participations in use cases*
Vertical plane	*Identity*	Decentralized identifiers	X	X	X	X	X	X	X	7
		eSIM	X	X	X	X	X	X	X	7
		Biometrics	X				X			2
		Authentication	X	X	X	X	X	X	X	7
	Trust	Verifiable credentials	X	X	X	X	X	X	X	7
		Authorization	X	X	X	X	X	X	X	7
		Reputation Systems	X	X	X	X	X	X	X	7
		Attestation	X		X	X	X	X	X	6
	Recovery	Self-recovery						X	X	2
		Credentials Recovery	X					X	X	3
Horizontal plane	*Privacy*	Self-aware data privacy	X		X	X	X			4
		Federated AI						X	X	2
	Security	Behaviour Monitoring	X	X	X	X	X	X	X	7
		Flow Monitoring								0
		Cyber Threat Intelligence	X	X	X	X	X	X	X	7
		Self-Healing								0
		IoT infrastructure self-protection								0
		IoT device self-protection						X	X	2
	Common	Hardened Encryption	X	X	X	X	X	X	X	7
		Permissioned blockchain	X					X	X	3

Figure 6 - Domain A Technology Articulation Map

Regarding the project KPIs, the ability to measure these indicators depend on the implementation of all the components foreseen in ARCADIAN-IoT concept and objectives. To understand the components participation in the use cases and understand if all have an active role, was built a *Technology Articulation Map*, a tool that maps the application of each component in each use case for the three domains. Figure 6, Figure 7 and Figure 8 show the *Technology Articulation Map* for

domains A, B and C respectively, and Figure 9 presents the consolidated view of the use cases usage in the 3 domains.

Domain B: Secured early monitoring of grid infrastructures			Use Cases						
			B1	B2	B3	B4	B5	B6	
			New device registration	GMS IoT device data gathering and transmission process	Service request from third-party IoT monitoring platforms	GMS IoT device security or privacy incident	GMS middleware security or privacy incident	External data audit to grid infrastructure	*Number of component participations in use cases*
Vertical plane	*Identity*	Decentralized identifiers	X	X	X	X	X	X	6
		eSIM	X	X	X	X		X	5
		Cryptochips	X	X	X	X			4
		Biometrics							0
		Authentication	X	X	X	X	X	X	6
	Trust	Verifiable credentials	X		X	X	X	X	5
		Authorization	X	X	X	X	X	X	6
		Reputation Systems	X	X	X	X	X	X	6
		Attestation	X			X	X		3
	Recovery	Self-recovery				X	X		2
		Credentials Recovery	X			X	X		3
Horizontal plane	*Privacy*	Self-aware data privacy	X	X		X		X	4
		Federated AI				X	X		2
	Security	Behaviour monitoring	X	X	X	X	X	X	6
		Flow Monitoring							0
		Cyber Threat Intelligence	X	X	X	X	X	X	6
		Self-Healing							0
		Self-Protection							0
	Common	Hardened Encryption	X	X	X	X	X	X	6
		Permissioned blockchain	X			X	X		3

Figure 7 - Domain B Technology Articulation Map

Domain C: Medical IoT			Use Cases							
			C1	C2	C3	C4	C5	C6	C7	
			MIoT kit delivery - Patient registration and authentication	MIoT capturing and sending vital signs and perceived health status	Personal data processing towards health alarm triggering	Monitor a patient and update a patient monitoring protocol	Patient MIoT devices security or privacy incident	MIoT Cloud services security or privacy incident	Medical 3rd party security or privacy incident	*Number of component participations in use cases*
Vertical plane	*Identity*	Decentralized identifiers	X	X		X	X	X	X	6
		eSIM	X	X		X	X			4
		Biometrics								0
		Authentication	X	X		X	X	X	X	6
	Trust	Verifiable credentials	X	X		X	X			4
		Authorization		X	X	X	X	X	X	6
		Reputation Systems	X	X	X	X	X	X	X	7
		Attestation	X	X			X	X	X	5
	Recovery	Self-recovery					X	X	X	3
		Credentials Recovery	X				X	X	X	4
Horizontal plane	*Privacy*	Self-aware data privacy	X	X	X	X	X	X	X	7
		Federated AI					X		X	2
	Security	Behaviour monitoring	X	X	X	X	X	X	X	7
		Flow Monitoring					X	X	X	3
		Cyber Threat Intelligence	X	X	X	X	X	X	X	7
		Self-Healing					X	X	X	3
		IoT infrastructure self-protection					X	X	X	3
		IoT device self-protection					X	X	X	3
	Common	Hardened Encryption	X	X	X	X	X	X	X	7
		Permissioned blockchain	X				X	X	X	4

Figure 8 - Domain C Technology Articulation Map

These maps show all the components of ARCADIAN-IoT framework have an active participation in the set of defined use cases. Therefore, we assume that the set of use cases is **complete** and form

a solid ground for components to address the intended KPIs (each component KPIs is presented in D2.4) in the research process.

Considering the co-creation strategy, joining IoT domain/solutions' experts, end-users and technology experts (academia, SMEs and industry) we assume that the use cases are **relevant and meaningful** to their IoT areas of actuation. Moreover, as shown in next sub-section (5.4.1), the relevance of the current use cases was also validated with external end-users, further validating its importance.

			Components participation in use cases per domain			Number of domains of application	Volume of application
			A	B	C		
Vertical plane	*Identity*	Decentralized identifiers	7	6	6	3	19
		eSIM	7	5	4	3	16
		Criptochips	0	4	0	1	4
		Biometrics	2	0	0	1	2
	Trust	Authentication	7	6	6	3	19
		Verifiable credentials	7	5	4	3	16
		Authorization	7	6	6	3	19
		Reputation Systems	7	6	7	3	20
		Attestation	6	3	5	3	14
	Recovery	Self-recovery	2	2	3	3	7
		Credentials Recovery	3	3	4	3	10
Horizontal plane	*Privacy*	Self-aware data privacy	4	4	7	3	15
		Federated AI	2	2	2	3	6
	Security	Behaviour Monitoring	7	6	7	3	20
		Flow Monitoring	0	0	3	1	3
		Cyber Threat Intelligence	7	6	7	3	20
		Self-Healing	0	0	3	1	3
		IoT infrastructure self-protection	0	0	3	1	3
		IoT device self-protection	2	0	3	2	5
	Common	Hardened Encryption	7	6	7	3	20
		Permissioned blockchain	3	3	4	3	10

Components w/ participation in:		
3 domains	15	71%
2 domains	1	5%
1 domain	5	24%

Figure 9 - Consolidated view of ARCADIAN-IoT components participation in use cases

In terms of **coherence**, we relate this attribute with the components ability to be agnostic to the IoT domain, having a coherent technical approach that allows the technology application to several IoT usage scenarios. As shown in the upper-right side of the table above, 76% of ARCADIAN-IoT components apply to more than one IoT domain and 71% apply to the three. Furthermore, patterns of usage and of articulation between ARCADIAN-IoT components are visible in the use cases' description, sometimes in the three IoT domains. These relations will just be formalized in D2.5, but these patterns indicate that the consortium didn't only achieve the seamless application of the trust, security and privacy management features in the project specific cases, but is starting to define a tangible framework where components are agnostic to the IoT domain and prepared to be used in many other IoT contexts.

5.4.1 Validation with external end-users' perspective

As described in the step 6 of the research methodology (section 3), despite the complete set of IoT agents present in the consortium, the unbiased perspective about privacy management, security, and trust from external end-users/stakeholders is a valuable asset to confirm the envisioned directions. With that in mind, five surveys were created targeting: (1) potential users of a drone vigilance service for Domain A; (2) grid infrastructure managers for Domain B; (3) potential patients using health monitoring IoT devices and (4) medical staff (e.g., doctors, nurses, other staff) for Domain C; and (5) cybersecurity experts for the CTI component. The surveys were disseminated through the social networks of the consortium and with direct invites done by the partners to the appropriate end-users. The first publication of the initiative was on the 21st of October and the results and findings reflect the state of the surveys on the 3rd of December.

Overall, there were 76 participations, 31 for Domain A, 1 for Domain B, 25 for Domain C Patients, 11 for Domain C Medical Staff and 8 for CTI component. The low participation in Domain B survey was due to the very specific, and hard to get, target audience (grid infrastructure managers). However, as result of the efforts done, the partner expert in this domain, BOX2M, already secured the participation of at least 5 grid/infrastructure companies who are willing to validate the project outcomes and inform regarding their perspective (to happen in WP5). Also, the number of medical staff and cybersecurity participants was not optimum due to being also a quite specific target audience, and efforts to engage more participants in next end-user initiatives will happen in WP5.

Below we describe the key findings for the surveys, excluding Domain B whose users will be targeted in a forthcoming stage.

Key findings A – Potential users of a drone service of vigilance and emergency (Domain A)

- The majority of the inquired do not feel that their personal device data is **private and only accessible by them** (81%), nor they feel that their **digital identity is well-managed and secure** (61%).
- 84% of the answers claim that it is critical or very important **to have control over their private data**.
- All the respondents trust more in systems that use **more than one authentication factor**.
- 81% of them claim to be critical or very important to have a **secure hardware component for identity and credentials storage**.
- 81% of the inquired claim to be important or very important for the system to have the ability to **assess the integrity of personal devices**, in order to better protect the users, the platform, and the service, **against attacks and hacking**.

As the results demonstrate, these IoT end-users stress the need to strengthen their devices trustworthiness, security and privacy management technologies, stating the significance that they give to have control over their private data. Participants were positive regarding using more than

one authentication factor and in using secure hardware elements for storing sensitive data like their identity or authentication credentials. Participants confirmed also the importance of having a system able to assess their devices integrity and security, and protecting them against attacks and hacking.

Key findings C1 – Potential patients using medical IoT (Domain C)

- Aligned with the previous IoT users, the majority of the inquired do not feel that their personal device data is **private and only accessible by them** (68%), nor they feel that their **digital identity is well-managed and secure** (52%).
- 88% of the inquired claim that it is critical or very important **to have control over their private data**, all of them (100%) claim that it is critical or very important to **not have credentials vulnerable**, and also claim (100%) that is critical or very important to **not have personal data (e.g., health data) vulnerable**.
- Most respondents (96%) trust more in systems that use **more than one authentication factor**.
- 72% of the answers claim to be important or very important that **medical data is not sent** to entities **other than their own health service provider**.

In line and reinforcing the other IoT end-users perspective, the potential users of a medical IoT monitoring solution also confirmed the need to enforce security, privacy and trust technologies in the involved devices. All of them value the security and privacy of their personal health data as a critical or very important aspect, and confirmed the relevance of ensuring that only authorized medical staff accesses their data. These participants showed also more trust in strong authentication mechanisms that use more than one factor.

Key findings C2 – Medical staff that can potentially be monitoring patients with Medical IoT (Domain C)

- 91% of the respondents claim **data trustworthiness** to be critical or very important in **monitoring patient health data**.
- All (100%) claim to be critical or very important to be sure that they are not receiving data from a **fake medical device** or that a malicious device isn't acting with a **fake identity**.
- Equally, 100% of the answers claim that is critical or very important to be sure of the **identity of people sending data to the health system** and it is also critical or very important to assure that the **medical data isn't being accessed without permission**.
- 91% of the answers consider critical or very important to guarantee that **the patient smartphone** (i.e., the IoT bridge to get the medical data) **is not damaged or altered in an unauthorized way**.

The 11 representatives of the medical staff strongly manifested the importance of not having tampered data in the monitoring of patients. Being able to trust the IoT devices and the received data is seen as key in a solution such as the one proposed for monitoring patients at home using

IoT devices. Also agreed with the potential patients regarding the need to ensure that medical data isn't accessed without permission.

Key findings D – Cybersecurity professionals (Cyber Threat Intelligence component)

- When asked about the three most frequent IoT related incidents that they detect/solve daily, the respondent's top answers were **IoT-based data breaches** (62.5%), **Hijacking IoT devices** (62.5%) and **Botnet attacks** (50%).
- During their daily work, **investigating** and **analyzing incidents** is the most time-consuming technical task (50%).
- Regarding the tools to respond to IoT security/privacy incidents that they consider missing in their daily work, a **dynamic management of authorization based on devices/consumers reputation** gathered 75% of the votes and a **self-recovery system** gathered 50%.
- Similarly, when asked about what kind of IoT related threat intelligence they would like to have, both a **threats dashboard** and a **security reputation dashboard** gathered 62.5% of the votes, each.

The potential stakeholders of the CTI component view over the top IoT incidents focused on: data breaches, devices hijacking and botnet attacks. Investigating and analysing incidents is quite time consuming for these professionals, which shows the need for novel automatic tools for decision support. Cybersecurity professionals would value to have dynamic management of authorization based on devices reputation (trustworthiness) and a self-recovery system, which enforces the importance of ARCADIAN-IoT components. Dashboards with IoT threats and security reputation were also valued.

These results, gathered with 76 participants of several types, confirm the importance of most of the use cases and technical components brought by ARCADIAN-IoT at the eyes of potential end-users of the project outcomes.

6. PLANNING USE CASES IMPLEMENTATION

The use cases implementation will happen in WP5, specifically in T5.2, T5.3 and T5.4, led by the IoT domain/solution owners, LOAD, BOX2M and RGB respectively. Those tasks start immediately after task 2.1's conclusion, which means that there will be a continuous flow of work, from the use cases' specification to their implementation. The implementation will be the base for the validation of ARCADIAN-IoT framework objectives, allowing not only the to prove the overall goals, but also to assess the specific KPIs for each component (defined in D2.4) applied and demonstrated in concrete domains / environments.

The approach for the implementation of the use cases will be iterative, having several envisioned phases. Research, development, and assessment iterations will happen within each phase and in the overall implementation approach itself, which will iteratively increment features towards the final solutions, from the compliant hardware and UX artifacts design, to the operational IoT solutions integrated with the ARCADIAN-IoT framework.

Phase 1 [M8-M12] – Preparation of the three IoT solutions for ARCADIAN-IoT framework

In this phase, T5.2, T5.3 and T5.4 participants will use as input the use cases defined in this deliverable (D2.2) for preparing aspects for which no additional research will be needed, e.g., the IoT hardware of the solutions, designing the first UX artifacts for the interfaces, as well as preliminarily designing backend/Cloud services specific for each domain. All of these can start being developed by the IoT solution experts, with the support of the other task participants.

This phase of preparation for implementation, and of actual realization of IoT solution parts that do not depend on the framework components, leads to a second stage that considers the first deliverables of WP3 (D3.1; D3.4; D3.7; D3.10 and D3.13) and WP4 (D4.1; D4.4 and D4.7) from M12, when ARCADIAN-IoT component details should be known.

Phase 2 [M13-M20] – Incorporating first ARCADIAN-IoT components

According to the details provided in the first deliverables of WP3 (D3.1; D3.4; D3.7; D3.10 and D3.13) and WP4 (D4.1; D4.4 and D4.7) related to each ARCADIAN-IoT component (M12), in this phase those core technologies of the project will start being integrated in the IoT solutions. The first ARCADIAN-IoT prototype is expected at month 20 (milestone M3), which means that, by the end of this phase, components will have functional features at a readiness level that allows their partial application and validation in the use cases implementation. This first integrated experimentation of the ARCADIAN-IoT components will allow the consortium to learn and iterate in the use cases specification as needed, according to technical feasibility, end-user input, or other factors.

Phase 3 [M21-M24] – Final use cases integrating ARCADIAN-IoT framework

The first ARCADIAN-IoT framework prototype is expected to define consistently the framework I/O communications, which means that the APIs between devices, people and services with the framework are expected to be considerably stable. This means that, after this phase, the project is entering in its last year and the purpose is expected to be more focused in enhancing KPIs than on creating new features – however, this may still be the case for components whose assessment show the need for different approaches or different features that are feasible within the project period.

In this sense, between months 21 and 24 the use cases implementation will have the purpose of building stable IoT solutions (third-party compliant devices, services, apps, interfaces for people) that use ARCADIAN-IoT framework. These solutions will be ready for, in the next phase, coping with changes to the ARCADIAN-IoT components' KPIs with minor to no changes needed. In this phase the final IoT solutions are delivered (D5.3) and are target of the first formal validation (D5.4).

Phase 4 [M25-M36] – Use cases as test and validation vehicle

While some components are being enhanced according to the first formal validation results, this final phase aims to apply the use cases implementation from the previous stage to test and validate the final prototype of the ARCADIAN-IoT framework, due on month 30 (milestone M4). This encompasses the several types of tests needed to perform the final evaluation of the project objectives in M36 (D5.5) according to the KPIs defined.

7. LEGAL, ETHICAL, REGULATORY AND SOCIAL DIMENSIONS

Among the use cases, the most critical from the data protection standpoint are the ones involving drones and facial recognition (Domain A), as well as the one involving medical IoT and minors (Domain C). Domain B, related to grid infrastructures doesn't present particular data protection issues, since it will not involve personal data, but only aggregated data, completely disjointed from the subject.

7.1. IoT and data protection

ARCADIAN-IoT Project involves the use of different types of technologies and, in particular, of Internet of Things ("**IoT**") devices, collecting and processing different categories of personal data. This raises numerous data protection issues and potential challenges that need to be assessed and addressed.

The use of such technological components (*i.e.*, blockchain, AI, biometric technologies and IoT medical devices and drones) might raise issues on data protection, some of which have already been assessed in the deliverable D2.4 with the requirements for ARCADIAN-IoT framework.

Keeping in mind the requirements outlined in deliverable D2.4, this section is aimed at providing general considerations in relation to IoT devices and their integrations with blockchain and AI technologies, and then issue specific information in relation to the different IoT technologies used within ARCADIAN-IoT Project (*i.e.*, medical IoT devices and drones).

7.1.1 IoT and data protection challenges

The concept of IoT refers to infrastructures designed to record, process, store and transfer an extensive amount of data while interacting with other devices. Thus, IoT devices constantly collect vast amounts of data - such as location and health data - that relate to identified or identifiable natural persons and, therefore, qualifies as personal data pursuant to Article 4, paragraph 1, no. 1 of the Regulation (UE) 2016/679 (the so-called "**GDPR**").

The processing of personal data in this context also implies the coordinated intervention of different Partners involved in the development of IoT technologies, to provide functionalities or interfaces.

In the light of the above, the development of IoT raises significant privacy issues and challenges, already identified by the Article 29 Data Protection Working Party (now, the European Data Protection Board, "**WP29**" or "**EDPB**") in its Opinion 8/2014 on the "*Recent Developments of the Internet of Thing*". In particular, according to the Opinion, the following major risk categories can be identified:

1. **lack of control and information asymmetry**: as a result of the need to provide pervasive services, users might be under third-party monitoring and can lose all control on

dissemination of their data, depending on the data controller's level of transparency in relation to the data process;

2. **quality of users' consent**: the information asymmetry above mentioned constitutes a significant barrier to demonstrating a valid (*i.e.*, informed and freely given) consent under Article 7, GDPR. Moreover, classical mechanisms used to obtain individual's consent may be difficult to apply in IoT, resulting, according to the WP29, in a "low-quality" consent given in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the actual preferences of data subjects;
3. **intrusive bringing out of behaviour patterns and profiling**: even though different objects will separately collect isolated pieces of data, further analysis can reveal specific of data subjects' life such as habits, behaviours and preferences;
4. **interferences derived from data and repurposing of original processing**: apparently insignificant data originally collected through an IoT device (*e.g.*, accelerometer or gyroscope) and, in general, the amount of data generated by the IoT, may lend to secondary uses.

In addition to the above-mentioned concerns, the heterogeneous nature of the IoT and its critical use make cybersecurity an essential aspect, that is even more important when considering that every IoT developer deals with supply chain activities aiming at transforming raw materials and components into a finished IoT product. In this context, it is therefore essential to identify and implement privacy by design and by default measures.

It is important to note that given the complexity of the IoT threat landscape, the European Union Agency for Cybersecurity ("**ENISA**") addressed cybersecurity challenges related to the security of IoT devices adopting several provisions such as the "*Guidelines for securing the Internet of Things*" published in November 2020. In particular, the Guidelines identifies the security threats affecting IoT, lists and describes good practices and security measures as well as guidelines to ensure a comprehensive understanding of the security in the IoT supply chain (including the application of the GDPR and/or any other local regulation to cover risks associated with standards/regulations non-compliance).

7.1.2 Blockchain in IoT

In brief, blockchain is a decentralised system (*i.e.*, there is no master computer managing the entire chain), keeping a record of an ever-growing set of data. Given that the database can only be extended and previous records cannot be changed, blockchain technologies are deemed immutable and secure.

As pointed out in the previous paragraph, IoT presents security concerns that can be addressed by the blockchain.

In particular, the use of a private permissioned blockchain system (*i.e.*, special-purpose blockchain implementation that only works within a given system) provides immutable auditability and traceability properties to the data under management.

However, while securing the processing of users' personal data, the use of blockchain involves risks in relation to the GDPR requirements. In particular, the "immutability" of the data, implied

in the very nature of the blockchain, constitutes a critical point of tension between such technology and the provisions of the GDPR such as, *inter alia*:

1. purpose limitation and data minimisations principles pursuant to Article 5 of the GDPR, specification principle, according to which personal data must only be collected for specified, explicit and legitimate purposes and shall be adequate, relevant and limited to what is necessary in relation to these purposes. In the case of blockchain technology, the problem arises because, once added to the database, the data will always continue to be processed;
2. the possibility of exercising rights that the GDPR grants to data subjects and which should always be exercisable by them, including the right to rectification (Article 16, GDPR) and the right to erasure (so-called "right to be forgotten" pursuant to Article 17, GDPR).

7.1.3 Using AI technologies in IoT devices

Artificial Intelligence ("**AI**") is a set of technologies that combines data, algorithms and computing power. As pointed out by the EU Commission in its "*White Paper on Artificial Intelligence*"[20], the latter is rapidly developing and is going to transform the pattern of society and the way people act in it, improving, for example, health care and increasing the safety of citizens.

In this regard, the European Parliament has pointed out that the increasing use of AI systems also entails risks, including threats to fundamental rights, including:

1. risk that a bias (unconsciously set by the programmers) negatively influences machine learning and then affects the AI results (*e.g.*, the AI could "make decisions" influenced by ethnicity, gender, age, *etc.*);
2. opacity of the algorithms: the steps through which the data are interpreted are not always explainable (transparent);
3. privacy and sharing of data, given that the AI feeds on data which is indispensable for the training of the machine;
4. consent and autonomy: the data subject must be adequately informed of the technology and of the developments it may have. Moreover, the comprehensibility of what is being communicated must be guaranteed.

Back in 2018, the European Commission set out its vision of ethical, safe and state-of-the-art AI "made in Europe". To support the implementation of this vision, the Commission has set up a High Level Expert Group on Artificial Intelligence, which has developed the "*Ethics Guidelines for Trustworthy Artificial Intelligence*"[21], with the aim of promoting trustworthy AI. Starting from a fundamental rights-based approach, the Group identifies ethical principles and values that must be respected in the development, deployment and use of AI systems.

In particular, the Group provides key indications (such as paying special attention to situations involving vulnerable subjects, taking appropriate measures to mitigate risks, *etc.*), as well as

[20] https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
[21] https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

indications on how to achieve reliable AI by listing seven requirements that AI systems should meet, namely:

1. human intervention and surveillance;
2. technical robustness and security;
3. confidentiality and data governance;
4. transparency;
5. diversity;
6. non-discrimination and fairness
7. social and environmental well-being;
8. accountability.

Finally, it should be noted that in the context of the European Strategy for AI, the European Commission published, last 21 April, a proposal for a Regulation on the European approach to AI, proposing a European legal framework on AI.

7.1.4 IoT medical devices and the processing of health data

As mentioned in the previous paragraphs, the IoT nowadays covers all everyday tools that have become smart with the technological evolution, incorporating smart sensors collecting a wide variety of information and transmitting it to the network. In medicine, this trend - so-called "digital health" - refers to sensors that detect real-time information from the human body (heartbeat, temperature, movement, *etc.*).

On one hand, digital health makes healthcare better, safer and more efficient, enabling new ways of management of individuals' health. On the other hand, however, the continuous monitoring of patients' conditions underlies many risks to their rights and freedoms (*e.g.*, in relation to the consequences of incorrect monitoring due to the collection of inaccurate, incomplete, ambiguous or contradictory data). The need to address such risks is even more important when considering that the use of medical IoT systems involves the processing of health-related data, which therefore fall into the special categories of personal data under Article 9 of the GDPR.

7.2. Drones and facial recognition mechanisms

From a perspective focussing strictly on data protection, drone operations can be classified into two main categories: purpose of the operation involving personal data processing, on one hand, and, on the other hand, operations whose purpose does not include the processing of personal data.

With specific reference to the first type of operations, it must be noted that drones are combined with applications such as cameras or video-cameras and might also record the images, through software to process the video images, which might have further applications (including high power zoom, facial recognition, behaviour profiling, movement detection, night vision, GPS systems processing the location of the persons filmed, *etc*). This implies the collection, recording, organisation, storing, use and combination of data allowing the identification of persons.

It must be noticed that regulations for the use of airspace apply in parallel with personal data protection regulation such as the EU Regulations 2019/947 and 2019/945, setting out the

framework for the safe operation of civil drones in the European skies through a risk-based approach.

In particular, this balance should take into account national security strategies and the necessity of not to step back in the protection of privacy and security of the individuals. This is a crucial issue as new technologies (and, among them, drones) may impact in several individual aspects.

This precondition and the potential clash between fundamental rights of the individuals and the necessity of the European Union and of the member States to monitor the emerging threats to security has guided the approach of ARCADIAN-IoT and its legal and ethical outcomes.

According to EU Regulations 2019/947 and 2019/945, there is no distinction between leisure or civil, commercial drone activities. What is relevant for the EU regulations is the weight and the specifications of the civil drone as well as the operation it is intended to conduct.

Regulation (EU) 2019/947, which is applicable since 31 December 2020 in all EU Member States, including Norway and Liechtenstein, caters for most types of civil drone operations and their levels of risk. It defines three categories of civil drone operations:

1. the "open" category (Article 4) addresses the lower-risk civil drone operations, where safety is ensured provided the civil drone operator complies with the relevant requirements for its intended operation. This category is subdivided into three subcategories, namely A1, A2 and A3. Operational risks in the open category are considered low, and, therefore, no operational authorisation is required before starting a flight;
2. the "specific" category (Article 5) covers riskier civil drone operations, where safety is ensured by the drone operator by obtaining an operational authorisation from the national competent authority before starting the operation. To obtain the operational authorisation, the drone operator is required to conduct a risk assessment, which will determine the requirements necessary for the safe operation of the civil drone(s);
3. the "certified" category (Article 6), in which the safety risk is considerably high; therefore, the certification of the drone operator and its drone, as well as the licensing of the remote pilot(s), is always required to ensure safety.

The regulation also emphasises that all drone operators and remote pilots must comply with European and national rules regarding privacy and data protection. The drone operations must be carried out with the minor interference with the privacy and personal data of individuals on the ground, and any personal data collected must be handled in compliance with the principles, requirements and individual rights laid down in the GDPR.

7.3. Processing of special categories of personal data under GDPR

As pointed out in the deliverable D2.4 and stated in the previous paragraphs, components processing special categories of personal data pursuant to Article 9, GDPR will also be used in ARCADIAN-IoT activities. This applies specifically to biometrics components identifying persons through face recognition AI and to health data processed by the IoT medical devices.

Both biometric and health data fall within the special categories of personal data regulated by the Article 9, GDPR which states that "*processing of personal data revealing racial or ethnic origin,*

political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" unless one of the conditions laid down in Article 9(2) is met and, in particular, if the data subject has given explicit consent or if the processing.

While processing this type of data, it is important to keep in mind that the risk-based approach of the GDPR requires data controllers to use greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination.

7.4. The involvement of minors

Particular protection is necessary when collecting and processing children's personal data, because they may be less aware of the risks involved. As mentioned in the introduction of section 7, this type of users can be targeted in domain C.

7.4.1 Protection of Childrens' data in the GDPR

GDPR provides guidance for specific circumstances and risks related to children when their personal data is collected and processed, emphasising the need for clear communication with children about the processing of their personal data and the related risks. Moreover, the GDPR recognises the possibility for children to exercise their data protection rights.

As mentioned, the GDPR requires data controllers and processors to implement higher standards of protection when processing children's personal data. In particular, Recital 38 states that "*children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply [...] when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child*".

Given that children merit specific protection, Recital 58 provides that "*any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*".

7.4.2 Legal bases for processing children's personal information

Under the GDPR, data controllers have an obligation to process personal data with a legal basis, irrespective of whether it belongs to a child or an adult. Article 6 of the GDPR sets out the six possible legal bases for processing personal data, *i.e.*:

1. performance of a contract or taking steps to enter into a contract;
2. compliance with a legal obligation;
3. protecting vital interests of a data subject or another person;
4. performance of a task carried out in the public interest or through official authority;
5. legitimate interests of the data controller or another party; and
6. the consent of the data subject.

In particular, under Article 6(1)(a) of the GDPR, processing is lawful if *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes*", consent that must be freely given, specific, informed and unambiguous made by way of a clear statement or affirmative action by the data subject.

While processing childrens' personal data, data controllers should ensure that the children is given a real choice over how their personal data is used and that they have the capacity to understand exactly what it is they are consenting to, relying on:

1. age;
2. any imbalance of power that might be inherent in their relationship with the child.

Finally, special restrictions apply where organisations provide online services: infact, Article 8 in combination with member States law sets limitations as to the minimum age at which online service providers can rely.

7.4.3 The exercise of children's rights under GDPR

The GDPR does not address when children should be able to exercise these rights for themselves. In general, children should be able to exercise their data protection rights, whether directly or with assistance/ representation.

On this point, please note that a child's right to the protection of their privacy is guaranteed also by Article 16 of the United Nations Convention on the Rights of the Child ("**UNCRC**"). Moreover, Article 18 of the UNCRC highlights the rights and responsibilities of parents or legal guardians as protectors and caregivers to ensure the best interests of their children and the previous Article 5 recognises that the responsibilities, rights and duties of parents and legal guardians to provide guidance in the exercise of the child's rights must be consistent with the evolving capacities of the child.

However, according to the Irish Data Protection Authority's guidelines "*Fundamentals for a child-oriented approach to data processing*", in addition to taking account of the aforementioned presumption, others factors shall be taken into consideration:

1. the age of the child: the closer the child is to the age of 18, the more likely it is that a data controller holding the child's personal data should deal directly with the child themself;
2. the nature of the personal data and the processing being carried out;
3. the nature of the relationship between the child and the parent or guardian (*e.g.*, the existence of court orders relating to parental access or responsibility child protection *etc.*;
4. the purpose for which the parents or guardians seek to exercise the child's data protection rights;
5. whether the child would consent to the parents or guardians exercising their data protection rights;
6. whether allowing the parents or guardians to exercise the child's data protection rights would cause harm/ distress to the child;
7. whether there are any sectoral rules or laws which apply to the particular context in which the parents or guardians are seeking to exercise the child's data protection rights.

7.5. Data protection: specific safeguards to be adopted during the pilots' operation

Deliverable D1.7 Ethics guides already identified safeguards to be applied during the project lifetime. However, in case of pilots' operation, additional attention should be paid for the following topics emerged during the analysis of use cases.

In general, the processing of personal data must comply with some specific principles. Namely, personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ("**lawfulness, fairness and transparency**");
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("**purpose limitation**");
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**");
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("**accuracy**");
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ("**storage limitation**');
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("**integrity and confidentiality**").

7.5.1 Proportionality and strict necessity

The criteria of proportionality and strict necessity principles must guide the consortium during the pilots' execution.

Therefore, processing of personal information should be limited to specific circumstances and circumscribed purposes of ARCADIAN-IoT.

7.5.2 Purpose limitation

According to the purpose specification principle, personal data must only be collected for specified, explicit and legitimate purposes, while the compatible use condition and the

minimisation principle require personal data not to be further processed in a way incompatible with those purposes.

This principle has to be taken into account even more in the case of blockchain technology, because, once added to the database, the data will always continue to be processed. Data controllers relying on blockchain technology should therefore clearly communicate to data subjects that they are using this technology and explain the related implications, such as the fact that the processing is not limited to the original operations.

7.5.3 Accuracy of personal data

With reference to all the personal data processed and, in particular, to biometric data used for facial recognition purposes and the health data processed by the IoT medical devices, it is necessary to take steps to ensure that facial recognition data are accurate.

With specific reference to biometric data, this can be achieved by, testing systems, identifying and eliminating disparities with regard to demographic variations in skin colour, age and gender and, thus, avoiding unintended discrimination as well as implementing back-up procedures in case of system failure if the physical characteristics do not correspond to the technical standards.

Furthermore, the possibility to update and rectify the data (in compliance with the principle of accuracy of the data) should be foreseen, as well as, once the purpose has been achieved, to delete the data in the light of the principle of limited storage.

7.5.4 Transparency and data subjects' consent

The essence of the transparency obligation is set out in Article 12 of the GDPR, providing that the controllers "*shall take appropriate measures to provide any information referred to in Article 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*". Moreover, the European Data Protection Board - in its Guidelines on Transparency under the GDPR adopted on 11 April 2018 - has emphasised the importance of transparency as a freestanding right for children.

In particular, Article 12 requires that the information must be:

1. concise, transparent, intelligible and easily accessible;
2. clear and plain language must be used. The requirement for clear and plain language is of particular importance when providing information to children;
3. in writing "or by other means, including where appropriate, by electronic means;
4. provided free of charge.

When identifying appropriate transparency measures for children, Partners shall:

1. use a clear and child-friendly language to explain exactly what it is that they are doing with their personal data, also considering non-textual measures such as icons;
2. consider using methods such as just-in-time notifications;

3. be easy to contact;
4. provide clear explanations as to data control and default settings.

Moreover, while developing and using facial recognition technologies, the goal of transparency shall be achieved by providing user-friendly privacy policies, easy-to-understand signage that indicates that a facial recognition technology is deployed in a specific space, *etc*.

Bearing in mind the various types of data subjects, categories of data and the technologies used, it is recommended to inform the data subjects with a specific privacy policy, and to obtain a written and explicit consent from them. The consent is also required for communicating these data to third parties where necessary and in the cases where an anonymization of the data is not technically possible or excessively expensive in respect of the economic capabilities of the data controller.

Moreover, with reference to the use of drones in the Domain A pilot execution, it is recommended that the ARCADIAN-IoT consortium identifies and limits the test to a specific area, in order to easier collect in advance people's express consent eventually depicted in the video taken by the drones. In addition, if the flight during the pilot will be in a working area, it is recommended to previously inform the employees with a specific privacy policy, and to obtain a written and explicit consent from them.

7.5.5 Technical measures and anonymisation

The GDPR, in the light of the accountability principle, has introduced the concepts of privacy by design and privacy by default.

According to Recital 78 of the GDPR "*In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, 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, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*".

Pursuant to Article 25, paragraph 2 of the GDPR "*the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*".

As provided by Article 5, par. 1, lett. f) - also reported above - the personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). In line with this

principle, the Article 32 provides that the appropriate technical and organisational measures shall be implemented to ensure a level of security appropriate to the risk, including *inter alia*, as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

With specific reference to pseudonymisation or, if possible, anonymisation of data, it is also worth remembering that the GDPR only applies to personal data: this implies that where data continues to be processed beyond its initial purpose, but only in an anonymised form, then this processing no longer falls within the scope of the GDPR. Therefore, another requirement could be the anonymisation of the data in such cases.

7.5.6 Ensure the exercise of data subjects' rights

GDPR provides data subjects - *inter alia* - with the following rights that the Partner must ensure during the Pilot:

1. the right of access, *i.e.,* to know if her data are processed and to obtain a readable copy in an understandable format. It is notably used to check data accuracy;
2. the right to rectification, *i.e.,* to modify, correct or update data concerning them to reduce the spread or use of inaccurate information;
3. the right to erasure, *i.e.,* to delete their data;
4. the right to restriction of processing temporarily;
5. the right to withdraw the consent previously provided;
6. the right to human intervention in relation to profiling or a decision solely based on automated processing.

With reference to components using blockchain technology, it is necessary to ensure that the citizens can exercise the data subject rights according to the GDPR, giving back the control to the data subject by letting her/him the choice to "remember" or "forget" their identifiers, in order to be compliant with GDPR and, in particular, to the "right to be forgotten" when the user stops using services (or upon request).

Moreover, while processing children's personal data, partners should keep in mind - in case of exercising one of the rights under the GDPR - the requirements mentioned in the previous paragraph 7.2.3.

8. CONCLUSIONS

This public deliverable depicts the work done in the task 2.1 of ARCADIAN-IoT. It shows the iterative process of discovery of the project use cases, the use cases final description, and the evaluation of the final set in terms of completeness, relevance and coherence. This work considered contributions from IoT solution providers, end-users, IoT industry with active CSIRTs, and technical research experts proposing trust, security and privacy management solutions. Complementing these perspectives were added the legal, ethical, regulatory, and social dimensions provided by the consortium legal expert.

Task 2.1 was carried out in close articulation with task 2.2, which iteratively extracted, from the use cases, the requirements for each ARCADIAN-IoT component, and with task 2.3, that considers task 2.1 outcomes to define the research roadmap and an overall architecture. Therefore, jointly with the other WP2 tasks, the use cases description sets the research context for the technical components of the framework (WP3 and WP4), and the means of demonstration and validation of the project objectives (WP5).

The result is a set of 20 use cases for the 3 IoT domains, thoroughly described envisioning an articulated application of ARCADIAN-IoT components. The use cases were assessed, justified, and considered relevant, coherent, and complete. All use cases consider the application of components from the framework, being therefore relevant for the project demonstration and validation. The overall set of use cases includes the application of all ARCADIAN-IoT components in different stages of the IoT solutions usage lifecycle. The settled use cases also allow to address all the project objectives and KPIs. Furthermore, it is possible to find a coherent application of each component across different domains, thus enforcing the vision of a holistic framework where the components are likely to have application in domains beyond the ones targeted in the project.

To further validate the use cases relevance and start involving external end-users, a set of surveys was issued to potential users of the technology. The outcomes of the initiative confirm the relevance of the project technology and allowed to refine the usage scenarios with the external end-users' perspective.

The research results shown in this document depict potential uses for each ARCADIAN-IoT component and the expected articulation between these elements in real IoT solutions. However, following the planned agile methodology, it is expected that, with the new knowledge being built in WP3 and WP4, and further involvement of end-users in validation initiatives, these usage scenarios are iteratively improved to better fulfil the project objectives and the stakeholders needs (e.g. end-users, CSIRTs and IoT solution providers).