4

End-to-end Security and Privacy by Design for AHA-IoT Applications and Services

Mario Diaz Nava[1], Armand Castillejo[1], Sylvie Wuidart[1], Mathieu Gallissot[2], Nikolaos Kaklanis[3], Konstantinos Votis[3], Dimitrios Tzovaras[3], Anastasia Theodouli[3], Konstantinos Moschou[3], Aqeel Kazmi[5], Philippe Dallemagne[4], Corinne Kassapoglou-Faist[4], Sergio Guillen[7], Giuseppe Fico[8], Yorick Brunet[4], Thomas Loubier[2], Stephane Bergeon[2], Martin Serrano[5], Felipe Roca[6], Alejandro Medrano[8] and Byron Ortiz Sanchez[9]

[1]STMicroelectronics, France
[2]Univ. Grenoble Alpes, CEA-LETI Minatec Campus 38000 Grenoble, France
[3]Information Technologies Institute, Centre for Research and Technology Hellas, Greece
[4]CSEM Centre Suisse d'Electronique et de Microtechnique SA, Switzerland
[5]Insight Centre for Data Analytics, NUI Galway, Ireland
[6]HOP UBIQUITOUS SL, Spain
[7]MYSPHERA, Spain
[8]Life Supporting Technologies-Universidad Politécnica de Madrid, Spain
[9]Televes SA, Spain

Abstract

The chapter aims at describing the cybersecurity and privacy methodologies and solutions that the architecture defined in the ACTIVAGE Large-Scale Pilot, and the corresponding implementation in nine *Deployment sites* should follow to secure the IoT system and protect the personal data from potential malicious cyber-attacks and threats. It further presents common definitions, methods and repeatable processes to analyse and address all potential threats in terms of cybersecurity and privacy that might occur during the exploitation phase of the project.

4.1 Introduction

The Internet and mobile revolution have transformed our world. The Internet of Things (IoT) has significantly emerged over the last few years, aiming to change our lives by forming a massive ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context to offer a variety of services. By 2020, market analysts expect between 20 and 50 billion connected devices in the world. With all the benefits originating from the use of IoT technology, also come a range of ever-increasing challenges and security threats including data manipulation, data theft, and cyber-attacks. For instance, the ransomware landscape has dramatically shifted in 2017 and organizations bore the brunt of the damage caused by new, self-propagating threats such as WannaCry and Petya. Most recently, a report from Symantec ISTR [1] revealed that there were 470 thousand ransomware infections in 2016 and 319 thousand in the first-half of 2017.

The threats and risks related to the Internet of Things devices, systems and services are of manifold and they evolve rapidly. With a great impact on citizens' safety, security and privacy, the threat landscape concerning the Internet of Things is extremely wide and evolves rapidly. Hence, it is important to understand what needs to be secured to develop sophisticated security measures to protect the IoT infrastructure. Information (or data) lies at the heart of an IoT system, feeding into a continuous cycle of sensing, decision-making, and actions. The billions of "things" can be the target of intrusions and interferences that might dramatically jeopardize personal privacy. Since IoT is seen as a key enabler for creating new services and improving overall quality of life, consumers need to have trust and confidence about their data being secured and protected, therefore, making the cybersecurity of IoT systems an essential part.

Currently, there are no official guidelines available for trust of IoT devices, in addition, there is no regulatory compliance defined for minimum-security requirements. Despite the existence of many security guidelines in general, the literature lacks primary guidelines to help adopt security measures and standards for the IoT systems.

The European Union (EU) is working on several fronts to promote cyber resilience across the EU. It published several proposals in a 'cybersecurity package' in September 2017 [2]. Furthermore, the EU set up the Large-Scale Pilots to deploy IoT systems in five main areas [3]. The main goals of these LSPs is to solve key practical issues such as interoperability, security and

privacy, business models, validation of IoT powered applications and services at large-scale, etc. In this context, this chapter reports the initial outcomes obtained from security and privacy performed in the ACTIVAGE project[1] [4]. These activities contribute into mainly two areas:

- Technological – a secure large-scale deployment of connected objects.
- Societal – related to the project context, which is to create a smart environment for the ageing well of elderly people allowing the collection of sensitive personal data.

As in ACTIVAGE, the experimentations will involve around 7,000 users across 9 *Deployment Sites* (DSs)[2], the consortium has a great concern when it comes to the security and privacy related challenges and an opportunity to resolve these issues with the help of large-scale validation and testing. Platforms using public communication infrastructure will interconnect many IoT devices, which are inherently weakly secured. Several services will process confidential data by requiring control over the propagation of access control in the spirit of the General Data Protection Regulation (GDPR) [5]. GDPR is a primary law regulating how companies/organizations protect EU citizens' personal data.

This chapter gives an overview of the end-to-end security and privacy impact analysis performed in order to provide actionable recommendations. The outcomes are in the shape of guidelines and framework related to the cybersecurity and privacy aspects. The security risk analysis is

[1]ACTIVAGE project is a key factor in the IoT for the "Active and Healthy Ageing" (AHA) domain producing evidence of the IoT value on fostering the deployment of AHA solutions in Europe, through the integration of advanced IoT technologies across the value chain, demonstrating multiple AHA-IoT applications at large-scale in a usage context, in real operational conditions. IoT for the AHA domain is a strategic element for the creation of dynamic ecosystems to answer and prevent the challenges faced by health and social care systems. Differently from other sectors, "AHA-IoT" services are provided to persons taken individually and it takes place across all domains, as persons live in houses, neighbourhoods, cities, rural areas, mountains and valleys, access to transport systems, drive cars, go to shopping centres, airports, theatres, etc. Persons are the most extraordinary producers of individual's data: production and consumption of personal data across domains has become the front-line of concern, data privacy, security, authentication, access consent, ownership, storage management. In summary, ACTIVAGE is an LSP that brings together the IoT and AHA communities to demonstrate the value of the first with respect to successful implementation of AHA solutions in terms of QoL for Citizens, Sustainability of Health and Social Care Systems and Economical and industrial Growth in Europe.

[2]A Deployment site is a city or a region in the European Union in where a full large-scale pilot is set.

conducted at each layer of an IoT system and its deployment procedure. The objective is twofold: to bring an awareness of the security risks to the stakeholders involved in each deployment site and the provision of solutions/recommendations – concerning the technologies and services to be deployed for security and privacy of the IoT infrastructure.

The chapter aims at describing the cybersecurity and privacy methodologies and solutions that the ACTIVAGE architecture and the corresponding deployment sites should follow in order to secure the IoT system and data from potential malicious cyber-attacks and threats. It further presents common definitions, methods and repeatable processes to analyse and address all potential threats in terms of cybersecurity and privacy that might occur during the exploitation phase of the project. The whole process takes into account:

- Typical cybersecurity and privacy risks due to the IoT context.
- DSs particularities in terms of cybersecurity needs (e.g. data relevance).
- Relevance and effectiveness of cybersecurity and privacy mechanisms already foreseen by the DSs security managers.

In this work, an IoT system is divided into four layers (domains): device, gateway, cloud and application. The security and privacy analysis is performed throughout the entire system starting from the device domain to the application domain. It also considers the overall system life cycle, i.e. the analysis process is applied not only for the operation phase but also at configuration, installation, maintenance and removal phases.

The rest of the chapter is organized as follows. Section 4.2 presents the global objectives and requirements for cybersecurity and privacy in the context of AHA-IoT ecosystem. Section 4.3 presents the main recommendations on Cybersecurity and Privacy in IoT. Sections 4.4 and 4.5 present the methodologies undertaken for security and privacy and the recommendations in this context. Section 4.6 illustrates, through example use cases, some security and privacy solutions harnessed from the top-down approaches and their associated recommendations. Finally, Section 4.7 concludes this chapter.

4.2 Global Objectives and Requirements

4.2.1 Security

In an information system, the key objectives and requirements are defined to prevent unauthorized access, use, disclosure, modification, or removal of important data or information. CIA (Confidentiality, Integrity and

Availability) triad is a common and globally accepted model that is used to secure important information. The main cybersecurity objectives [6, 7] are:

- *Confidentiality*: no improper disclosure of information.
- *Integrity*: no improper modification of information (alteration, deletion or creation).
- *Availability*: no improper impairment of functionality.

In order to reach above objectives, the typical cybersecurity properties or requirements are listed as follows:

- *Authorization*: the rules on who is allowed to read, modify or delete which information.
- *User and entity authenticity*: the assurance that the other party is the intended communication peer, no "man-in-the-middle" scenario.
- *Integrity* (*data and service authenticity*): the data is not altered during transmission (accidentally or intentionally).
- *Confidentiality*: the exchanged data cannot be overheard or made available to a third party.
- *Timeliness and validity of the data*: for example, protection against message replay.
- *Non-repudiation of the transaction*: the assurance that a transaction is auditable.

In addition, system integrity requirements include a system protection against physical and logical attacks, a secure software update mechanism and the monitoring and reaction capability to system malfunction. The mechanisms to achieve these requirements are the following:

- *Access Control*: selective restriction of access to data or services.
- *Entity authentication*: for example, a cryptography-based "handshake" scheme.
- *Message cryptographic protection*: encryption and data authentication.
- *Temporization of data*: use of nonces, timestamps, counters against replay attacks.
- *Code signing*: use of cryptographic hash to validate authenticity and integrity of the code.
- *Cryptographic key establishment*: a scheme to allow key exchange between two parties.
- *OS and hardware security*: protection mechanisms such as root of trust, secure boot, etc.

Additional requirements on the cybersecurity solutions are scalability and usability, which focus on the identification and access control methodology combined with usability of human interfaces. Furthermore, the system management deals with the management of the keys, the configuration, installation, replacement of devices, and the monitoring and malfunction detection.

If security and privacy are already big challenges on IT systems, these challenges become much more important on the IoT systems considering that the attack surface has significantly been enlarged as well as the amount of data generated and handled [8]. Furthermore, the impact becomes more important considering that IoT devices have not enough processing capabilities, in contrast to IT systems, and they have a limited autonomy because they work most of the cases on batteries. They use generally different wireless connectivity solutions not compliant with existing security standards. Last but not the least, the nature of the applications, for instance AHA, requires a high level of security to keep end-to-end data integrity, confidentiality and service availability. The AHA users are very concerned by these aspects.

Secure IoT systems with high level of personal data protection are mandatory to keep the users' trust. These aspects are essential to deploy massively the IoT technologies in the coming years.

4.2.2 Privacy

Concerning the objectives and recommendations for the privacy this work uses the General Data Protection Regulation (GDPR) (EU 2016/679)[3] as the basis. In addition, the Data Protection Impact Assessment (DPIA) process is used to put in place such regulation. The article 1 of GDPR defines the following objectives:

- This Regulation lays down relating to the protection of natural persons with regards to the processing of personal data and rules relating to the free movement of personal data.
- This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

[3]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

The GDPR defines also the following requirements:

The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate legal, technical and organizational measures be taken to ensure that the requirements of this Regulation are met.

In order to be able to demonstrate compliance with this regulation, the data controller should adopt internal policies and implement measures that meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of:

- Minimizing the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Transparency regarding 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.

4.3 Recommendations on Cybersecurity and Privacy in IoT

4.3.1 Security

Security is a complex and critical concern for any manager of interconnected digital assets. Many private companies [9], public bodies [10] and standardization/harmonization institutes (e.g. RFC 2196 Site Security Handbook) have published recommendations aiming at improving the quality and consistency of the security levels across interconnected systems. Such recommendations target system managers, organization officers, service providers, infrastructure owners, product manufacturers, developers, end users and indirectly also attackers. In fact, as promoted by security experts, every security measure, mechanism and algorithm must rely on publicly available specifications. Recommendations are elaborated and publicized proactively [15, 11] and reactively [11]. Interestingly some of them are associated to supporting tools [10].

All these sets of recommendations present diverse facets of similar rules and recommendations. It is not possible to include the whole list in this chapter. However, recommendations insist on the fact that security is a continuous process with integrated improvement procedure, based on the continuous evaluation of the in-place security. Therefore, external inspection such as auditing is a must. Self-auditing and internal expertise are strongly required, but by far not enough. External companies

offer services to analyse the implemented security, including security standards, such as ISO/IEC 27001 and 27002, the NIST Cybersecurity Framework.

4.3.2 Privacy

When developing, designing and using applications, services and products that aim to process personal data to fulfil their task, the developers/producers of such products, services and applications are recommended to take into account the right to data protection. It is important to make sure that controllers and processors are capable enough to fulfil data protection obligations. Furthermore, the principles of data protection by design and by default should be also taken into consideration in the context of public tenders.

A report by ENISA (the European Union Agency for Network and Information Society) elaborates on what needs to be done to achieve privacy and data protection by default [13]. It specifies that encryption and decryption operations must be carried out locally, not by a remote service, because both keys and data must remain in the power of the data owner if greater privacy needs to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

In literature, there are additional principles and guidelines available that can be used to achieve privacy and data protection by default, also known as *privacy by design*. Privacy by design [14] is a concept, developed in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies (ICTs), and of large-scale networked data systems. The objectives of privacy by design – ensuring privacy and gaining personal control over one's information, and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following 7 foundational principles:

1. Proactive not reactive; preventative not remedial.
2. Privacy as the default setting.
3. Privacy embedded into design.
4. Full functionality – positive-sum, not zero-sum.
5. End-to-end security – full lifecycle protection.
6. Visibility and transparency – keep it open.
7. Respect for user privacy – keep it user-centric.

4.4 Security Approach

4.4.1 Methodology

To achieve the objectives defined above, a number of activities are performed to lay down the security and privacy policies in the context of ACTIVAGE project. For the purpose of security, activities include:

- Perform a reference risk analysis in the ACTIVAGE IoT environment in order to identify the general ACTIVAGE security requirements, which depend on the criticality of applications or services.
- Countermeasures to mitigate risks are identified at this stage.
- Create and elaborate the ACTIVAGE security questionnaire.
- Analyse questionnaires' responses and perform assessments for the DS' security requirements.
- Define the security cartography and recommendations for each deployment site.

The elaboration of the security questionnaire considered the following aspects:

- Collect relevant information allowing the identification of missing mechanisms to ensure full end-to-end cybersecurity and privacy for each of the DSs.
- Make it easy for the DSs security managers to reply. The DS security manager is in charge of the security and privacy aspects related to this DS.
- Make the DSs security managers aware of cybersecurity and privacy issues that have not yet been identified and support the other stakeholders to realize the high importance of these aspects that are critical considering the nature of the project, which includes data confidentiality, higher vulnerability by connecting "smart objects" to the system, etc.

Security analysis is performed based on the following assumptions:

- All IoT devices and elements constituting the DS meet safety requirements according to the existing norms and regulations in conformance to their original purpose. This falls into the responsibility of the device manufacturer or SW provider/service provider and of the DS manager. e.g., an electrical heater used to ensure the comfort of elderly people must respect basic norms for electrical heaters.
- DS security managers know the basic norms and regulations rules with which the devices, SW and services used must comply. The managers

should be able to provide the corresponding evidence and they should highlight any unconformity. Questionnaires take into account that the answers are given considering the country rules where the DS is deployed.

- Each of the service providers who plans to use the ACTIVAGE technology needs to upgrade and adapt the DS elements/settings/components to the norms and the regulations in force at the time and in relation to the location of the commercial exploitation.

The general risk analysis adopted the ACTIVAGE Reference Architecture shown in Figure 4.1 and was carried along the following typical steps:

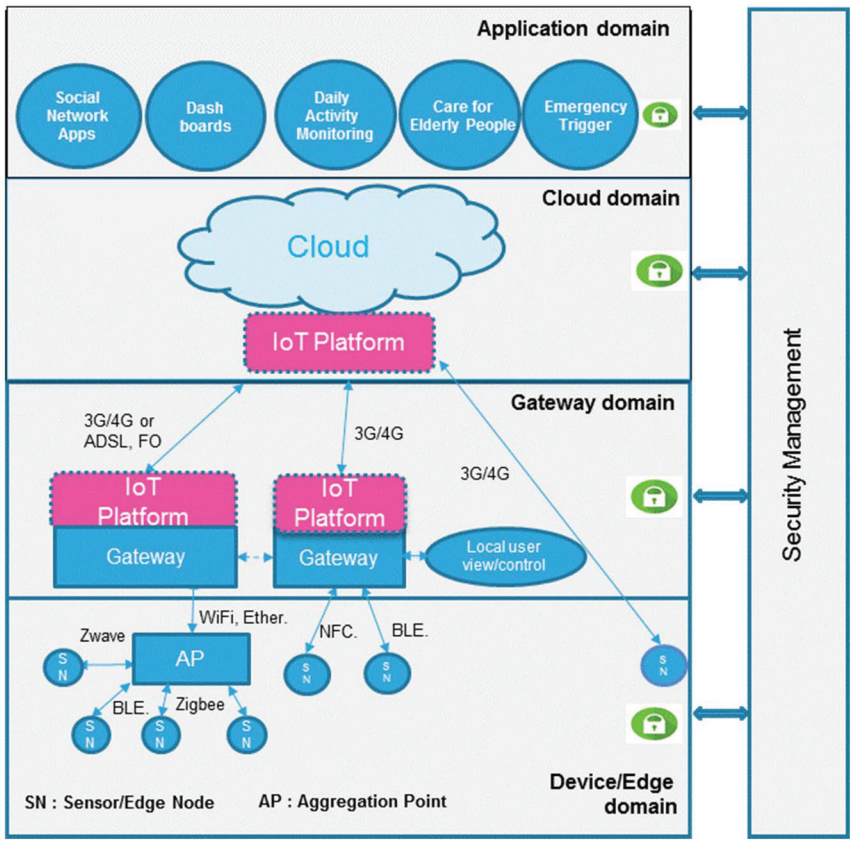

Figure 4.1 ACTIVAGE Reference Architecture.

- Identification and description of all the assets to be protected in the IoT system.
- Identification of all threats and vulnerabilities for each asset.
- Quantification of security risk caused by the threats and vulnerabilities, using a metric.
- Risk management: the decision on which risks to counter and which ones are acceptable.

The risk analysis leads to the definition of the appropriate security measures.

4.4.1.1 Assets identification and description

An Assets list was established as a guideline to be carefully analysed, completed (if needed) and used for each DS. It includes all data in the system, services, pieces of hardware, software, communication links and may be extended to intellectual property, brand reputation, buildings etc. The most important items in this list are given hereafter.

Data assets include application and management data. The typesets and formats should be defined in the data model.

Application data describe the elements or resources of the IoT system. They include, for example:

- Data describing all entities producing or consuming data (Identifiers and attributes of individuals, stakeholders, sensors).
- Data that are monitored and analysed by the IoT system in order to ensure the expected service (raw measurements, processed data elements).
- Decisions of the system that influence the subject's environment (guidance or prescriptions for individuals, environmental instructions for smart sensors, configuration instructions for devices).

Management data relate to system operation. They include, for example:

- Procedure, action plan descriptions (definition of all the planned actions in case of occurrence of an extreme event).
- Data storage organization definition (for example, a Grading Table, Detail Description predefines categories for data storage, such as Medical information, Medical report, Wellness information, Service, etc.).
- Access Rights Table, defining the access rights for each stakeholder profile.
- Transaction registers, logging the History of all operated transactions (communication channel, data, data user, time, etc.).

- Cryptographic material that may include log-in credentials, cryptographic secrets for authentication and encryption, root-of-trust information (e.g. trusted PKI public key), public key certificates, etc.

Assets also include hardware and software elements.

Communication channels. The connection between the devices and the IoT-Gateway is generally wireless (BLE, Z-wave; Zigbee, etc.). The connection between the IoT-Gateway and the Cloud can be an Internet connection. However, and many times, the IoT-Gateway is connected via Wi-Fi/Ethernet to a second Gateway that performs the Internet connection via 2G/3G/4G or a wired connection (XDSL, Cable, OF). On the application end, the connection between the user and the Cloud can be wired or wireless. The wired connection can be through the chain Lap and Desk Tops, LAN, Gateway. The Gateway allows connecting the user with the Internet network and this one to the Cloud. The wireless connection (2G/3G/4G) is done by having a direct connection between the Smart Phones and Tables directly to Internet having access to Web applications.

Component hardware. For example, typical hardware assets to consider at the low domains (Device and Gateway) are data storage units, processing units, power management blocks, sensing and actuating blocks as well as all device interfaces (e.g. I/O, JTAG ports, etc.) and device casing. Maturity and configuration must be assessed.

Component software and configuration information. Software must be analysed at all levels: OS, firmware, application embedded software, high-level application container. Boot mechanisms and system configuration at all IoT levels also need particular protection and are included in the assets list.

Trust associations (end-to-end security). Establishing an end-to-end security association, between the data source and their final destination, provides a higher and often necessary level of data protection. The data are not made available at any of the intermediate hops, since they are encrypted at their source and only the final data user is able to decrypt them.

4.4.1.2 Security risk analysis tools: Product or service compliance class, STRIDE, DREAD

The IoT Security Compliance Framework [15] and other guideline documents issued by the IoT Security Foundation are used to enhance best security practices during development and installation of an IoT product (or system or service). The Framework includes the definition of Compliance Classes for

products and a series of criteria in order to validate their security depending on the targeted class. Applicability of the requirements on a product depends on its compliance class, which is expressed as a number between 0 to 4, increasing with security level. To define compliance classes, three levels of risk impact, BASIC, MEDIUM and HIGH, are defined for each of the three security objectives, namely confidentiality, integrity and availability. For instance, MEDIUM confidentiality corresponds to "*Devices process sensitive information (including Personally Identifiable Information – PII); limited impact if compromised*" and is required from class 2.

The risk analysis methodology followed in ACTIVAGE to identify the threats is based on the STRIDE Methodology, see Table 4.1. This Threat classification model was developed by Microsoft [18, 19], and helps answering the question "what can go wrong in the system?"

The risk mitigation technologies (Cybersecurity measures or Cybersecurity controls) against a STRIDE threat to apply on the system element under consideration depend on the element type, perspective (developer, administrator) and assessed risk level (DREAD rate). Recommendations by foundations or standard bodies give guidelines in this task, providing lists of Cybersecurity requirements depending on risk level (or compliance class) as well as best-practice tips [16, 17].

In the case study described here below, we identify the Cybersecurity controls to apply to each system element and gives an indication of:

- The compliance classes for which the control must be applied.
- The applicability level, which is defined as **mandatory** (the requirement shall be met, as it is vital to secure the product category) or as **advisory** (the requirement should be met unless there are sound reasons such as economic viability or hardware complexity, in which case the reasons for deviating from the requirement must be documented).

Table 4.1 STRIDE

Threat	Concerned Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

4.4.1.3 ACTIVAGE as example of Risk Analysis

The Threat analysis is performed on **Device, Gateway, Cloud and Application** domains following the proposed IoT reference architecture. As an example, the STRIDE analysis applied to an IoT reference Device is detailed below.

Proposed Assets description of an IoT reference Device, see Figure 4.2:

- HW description, configuration integrity for IoT devices:
  - Connectivity (description and maturity): Communication Channel CC1
  - Processing (description and maturity): P1
  - Data Storage (description and maturity): DS1
    - Individual Subject id, Devices Id,
    - Raw Data (Individual Subject, Environmental, Devices and Services).
    - Processed Data (Individual Subject, Environmental, Devices and Services).
    - Instructions (Users, Environmental, Devices and Services).
    - Data grading table in (DS1) & Access right table in (DS1).
- In Device Data Flow (DF), the following analysis must be performed on:
  - Connectivity/Communication channels: BLE, Wi-Fi, LoRa, NB-IoT
    - Nature of Data: Individual Subject, Devices, Raw & Processed Data, Instructions (Users, Environmental, Devices & Services).

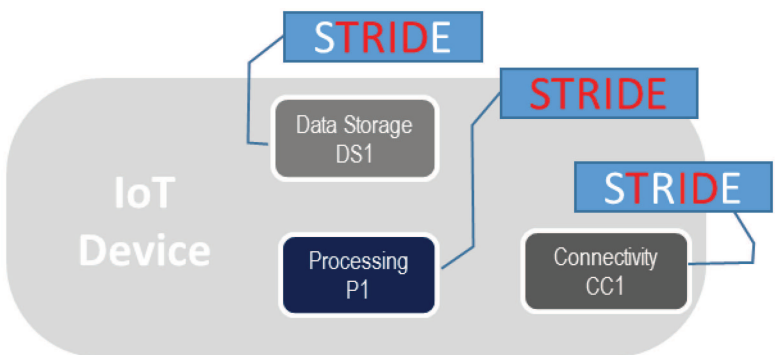

Figure 4.2 IoT device assets and STRIDE representation.

In this example, the threats concerning the related asset are identified in red bold characters in Figure 4.2:

- In DS1: Tampering, Repudiation, Information disclosure and Denial of service.
- In P1: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of Privilege.
- In CC1: Tampering, Information disclosure and Denial of service.

Subsequently, an evaluation of the vulnerability of the IoT Device is performed. The question to be answered is: "What will be the impact of the attacks on the assets?" All the threats for every element are rated using DREAD method ranked from 1 to 3 point, where the DREAD rate refers to all the risks as defined in Table 4.2.

Table 4.2 DREAD ranking definition

Risk	Risk Property	Description/point
Damage potential	How great can be the damage?	1pt (low): Leaking trivial information 2pts (medium): Leaking sensitive information 3pts (high): Can subvert the security system
Reproducibility	How easy to reproduce?	1pt (low): Very difficult to reproduce, even with knowledge of the security hole 2pts (medium): Can be **reproduced**, but only with a timing window and a particular situation 3pts (high): Can be reproduces every time and doesn't require any particular situation
Exploitability	How easy to realize this threat?	1pt (low): Requires an extremely skilled person and in-depth knowledge every time to exploit 2pts (medium): A skilled programmer could make the attack, then repeat the steps 3pts (high): A novice programmer could make the attack in a short time
Affected users	How many users are affected?	1pt (low): Very small % of users, obscure feature; affects anonymous users 2pts (medium): Some users, non-default configuration 3pts (high): All users, default configuration, key customer
Discoverability	How easy to find this vulnerability?	1pt (low): The bug is obscure, and it's unlikely that users will work out damage potential 2pts (medium): located in a seldom-used part, and only a few users should come across it 3pts (high): The vulnerability is located in the most commonly feature and is very noticeable

See below a DREAD ranking based of on the proposed case study.

Table 4.3 DREAD ranking evaluation and analysis

Threat Applicable	DREAD Rate Evaluation	Analysis
Spoofing	$2, 3, 2, 2, 1 \rightarrow 2$	Weak Password
Tampering	$3, 2, 1, 2, 1 \rightarrow 1.8$	
Repudiation	$1, 2, 2, 2, 1 \rightarrow 1.6$	
Information disclosure	$3, 2, 1, 2, 1 \rightarrow 1.8$	
Denial of Service	$3, 3, 3, 1, 1 \rightarrow 2.2$	Physical port accessible
Elevation of Privilege	$3, 2, 2, 1, 1 \rightarrow 1.8$	

The result of the assessment can be compared to the minimum requirement of compliance class. As soon as the weaknesses are identified, the strategy to address the risk must be explicitly detailed. Basic risk strategies are mitigation, acceptation or transfer to a third party.

Table 4.4 Basic strategy analysis

Threat Applicable	Risk	Strategy	DREAD Rate
Spoofing	Mitigate	Secure boot process	$2, 2, 2, 2, 1 \rightarrow 1.8$
Tampering	Accepted		$3, 2, 1, 2, 1 \rightarrow 1.8$
Repudiation	Accepted		$1, 2, 2, 2, 1 \rightarrow 1.6$
Information disclosure	Accepted		$3, 2, 1, 2, 1 \rightarrow 1.8$
Denial of Service	Mitigate	All non-used ports are physically inaccessible	$3, 2, 1, 1, 1 \rightarrow 1.6$
Elevation of Privilege	Accepted		$3, 2, 2, 1, 1 \rightarrow 1.8$

4.5 Privacy Approach

4.5.1 Introduction

Nowadays, Privacy in Europe has gained a lot of visibility through the advent of the new General Data Protection Regulation (GDPR) entered in force on May 25th, 2018 in the European Union. Until recently, companies making business out of personal or other types of data systematically pushed privacy back. Entities promoting the privacy preservation and enforcement processes propose different approaches. In this chapter, the authors propose to develop a general methodology on Privacy to define a privacy impact analysis for a given IoT System and provide recommendations and guidelines in order to minimize the Privacy threats. The complete methodology is described

hereafter. It is under deployment in the Deployment sites of the ACTIVAGE project.

Moreover, and in complement of the Security methodology described in Section 4.4, the authors made an analysis of the GDPR to identify the Privacy modules/services/articles that should be implemented in any IoT system of the ACTIVAGE project. This analysis allowed identifying some use cases that are well suited to be implemented using a Blockchain based technology, as described in the Section 4.6.3.

4.5.2 Methodology to Perform Privacy Analysis and Recommendations

Figure 4.3 shows the Privacy methodology proposed in order to perform risk privacy analysis on an IoT system. This is the methodology we have used in ACTIVAGE for this purpose. The expected outcomes are the identification of the countermeasures/recommendations for this IoT system to minimize the risks of privacy threats: data theft, data misuse or any other malicious usage. This methodology is addressed to any non-professional data protection manager to facilitate, him/her, the implementation of the GDPR regulation.

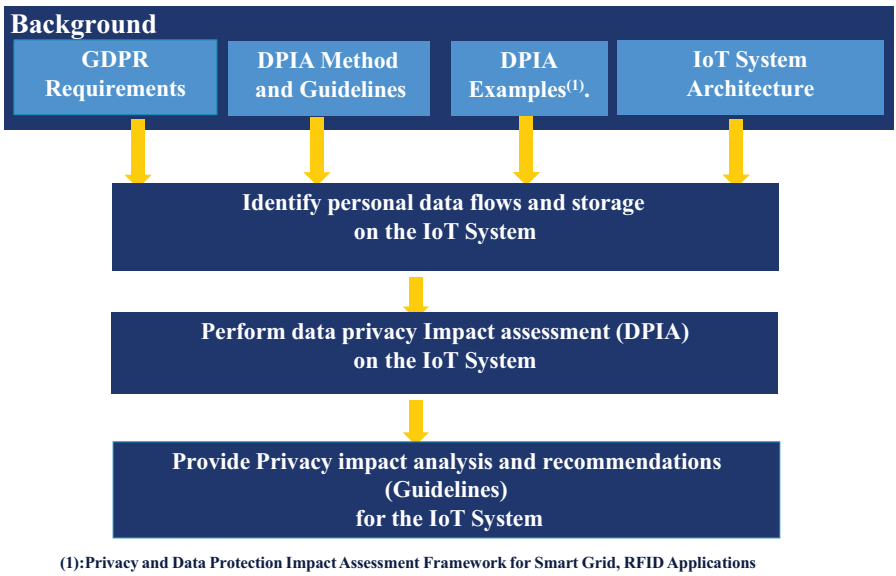

Figure 4.3 Privacy methodology.

This methodology consists in the execution of the following four main steps:

- **Background** – A good acknowledge of the following elements is required: What is the GDPR?

  What is a DPIA and how should be performed? What are the IoT System architecture and topology where the Data will be generated, stored, processed and exploited (and by whom) to identify security rights? In order to get the answers to these questions, the following documents are available [5, 20–24].
- **Identify personal data flow and storage** – For any IoT system, it is required to know its complete and detailed architecture and topology as discussed in Section 4.4. This information allows "easily" the identification of assets, data flows, data storage, process units, users, etc. and their location.
- **Perform Data Impact Performance Assessment** – (DPIA) This step is key in the methodology. The importance of this step and the way to develop it are described with more details in the next paragraph.
- **Provide Privacy Impact Analysis and Recommendations** – This step provides the DPIA analysis results of the IoT system under study and the recommendations proposed to deploy the system with good Privacy properties.

4.5.3 Data Protection Impact Assessment (DPIA)[4]

GDPR introduces the concept of a Data Protection Impact Assessment (DPIA)[5] [20] and strongly recommend carrying out one for each system concerned. This paragraph addresses the following questions: what is a DPIA?, when a DPIA is mandatory and how to carry it?, and what are the main elements containing a DPIA?

4.5.3.1 What is a DPIA?

"A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help managing the risks to the rights and freedoms of natural persons resulting from the processing of personal data. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to

[4]This information contained in this paragraph was extracted from [20].

[5]The term "Privacy Impact Assessment (PIA) is often used in other contexts to refer to the same concept", for more information see [21–23].

demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, *a DPIA is a process for building and demonstrating compliance*".

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA[6] can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

4.5.3.2 When is a DPIA mandatory?

Where a processing is "likely to result in a high risk to the rights and freedoms of natural persons". Table 4.5 gives some examples where a DPIA is required.

Table 4.5 Examples where DPIA is required

Examples of Processing	Possible Relevant Criteria	DPIA Required?
A hospital processing its patients' genetic and health data (hospital information system).	• Sensitive data • Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages using an intelligent video analysis system to single out cars and automatically recognize license plates.	• Systematic monitoring • Innovative use or applying technological or organizational solutions	Yes
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	• Systematic monitoring • Data concerning vulnerable data subjects	Yes
An online magazine using a mailing list to send a generic daily digest to its subscribers.	—	Not necessarily

4.5.3.3 When should the DPIA be carried out?

"*prior to the processing*". This is consistent with data protection by design and by default principles. The DPIA should be started as early as practical

[6]For instance, when the processing is subject to a DPIA, or carrying out a DPIA in an incorrect way, or failing to consult the competent supervisory authority where required.

in the design of the processing operation even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle project. It will ensure that data protection and privacy are considered and promote the creation of solutions that promote compliance.

4.5.3.4 What is the DPIA minimum content?

The GDPR does not formally define the concept of a DPIA as such, but it sets out its minimum features as follows:

- Its minimal content is specified as follows:
  a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.
  b) An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
  c) An assessment of the risks to the rights and freedoms of data subjects.
  d) The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
- Its meaning and role are clarified: "In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".

Figure 4.4 illustrates the generic iterative process for carrying out a DPIA. It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed. Furthermore, this process should be regularly performed to evaluate the IoT system evolution over the time.

Practical recommendations (necessary but not sufficient) when carrying out a DPIA

The basic recommendation is to collect only required personal data to minimize the risk of non-compliance. It excludes the "just in case" approach in

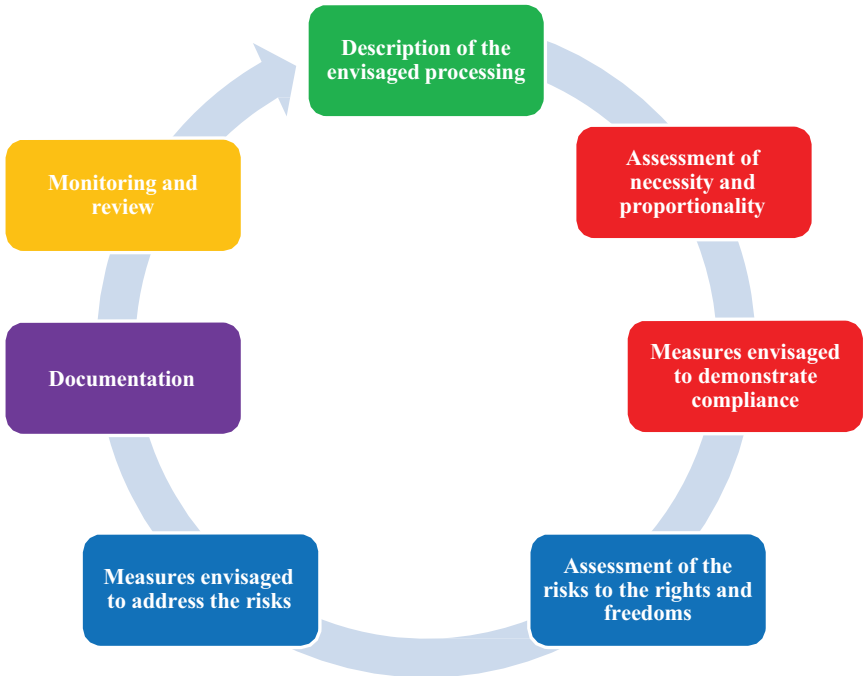

Figure 4.4 Process for carrying out a DPIA.

which unjustified data is collected for future uses, even when they may be justified.

It requires a complete audit of the data already in possession of the various stakeholders (processors, etc.), and the data must be kept based on the principle of usefulness for the subject and necessity for the service.

4.5.4 GDPR Analysis for Implementation

To cope with GDPR in an IT system and more particularly on IoT based system (as such foreseen in ACTIVAGE where security and privacy are of high importance according to AHA applications supported), a first analysis was performed on the set of articles constituting the GDPR. They were analysed and classified as follows:

- Legal: Articles related with legal issues.
- Technical: Articles requiring a technical implementation.

- Accountability: Articles related to the organization/company Governance.
- Principles: Articles providing recommendations to be considering in the GDPR implementation.

Table 4.6 gives the details of this analysis. It is composed of three columns indicating (from the left to the right): the type of article (Legal, Technical, etc.), the type of service and the article description concerned by the GDPR.

On top of this first analysis, Varonis[7] recommends focusing on the following technical aspects during the implementation phase to meet the GDPR [25]:

- **Data classification** – Know where personal data is stored on the IT/IoT system. This is critical for both protecting the data as well as following through on requests to correct and erase personal data.
- **Metadata** – With GDPR requirements for limiting data retention, basic information on when and why the data was collected are required, as well as its purpose. Personal data residing in IT/IoT systems should be periodically reviewed to see whether it needs to be saved for the future.
- **Governance** – GDPR highlights the need to get back to basics. For enterprise (or AHA data), this should include understanding who is accessing personal data in the AHA file system, who should be authorized to access, and limiting file permission based on users' actual roles – i.e., role-based access controls.
- **Monitoring** – The breach notification requirement places a new burden on data controllers. Under the GDPR, the IT/IoT security mantra should be "always be monitoring". Data protection controllers need to spot unusual access patterns against files containing personal data, and promptly report an exposure to the local data authority. Failure to do so can lead to enormous fines, particularly for multinationals with large global revenues.

The analysis performed in this section contributed to identify several Privacy uses cases to be implemented using the innovative and pervasive Blockchain as a potential technology to provide robust and efficient IoT solutions on security and privacy. The following section describes these developments.

[7]Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics.

Table 4.6 GDPR Analysis in view of its implementation

Type of Article	Provided Function or Service	GDPR Article
Legal/Principle		*Article 5 – Basic principles related to data Security*
Legal/Technical	Establish access controls and protected regulated data.	*Article 6 – Lawfulness of processing Subject's consent*
Legal/technical	Establish access controls and protected regulated data.	*Article 7 – Conditions for consumer Consent*
Legal/technical	Establish access controls and protected regulated data.	*Article 13 and 14 – Information and access to personal data*
Technical	Automatically discover and classify GDPR affected data	*Article 15 – Right of access by the data subject.* Enable to provide the data subject remote access to his or her personal data *Article 16 – Right to rectification* Be able to rectify specific data. *Article 17 – Right to erasure ('right to be forgotten').* Be able to discover and target specific data and automate removal *Article 18 – Right to restriction of processing* *Article 20 – Portability rights* Develop interoperable formats that enable data portability.
Technical	Audit and Traces control, protection against cyber-attacks and internal threats	*Article 30 – Records of processing activities.* Implement technical and organizational measures to properly process personal data
Technical	Establish access controls and protected regulated data.	*Article 25 – Data protection by design and by default.* Embrace accountability and privacy by design as a business culture • Collect only the required data • Give access only to the right people • Availability to prove and demonstrate
Legal/technical	Management of incidents and notifications	*Article 33 – Notification of a personal data breach to the supervisory authority*. Prevent and alert on data breach activity; have an incidence response plan in place

(*Continued*)

Table 4.6 Continued

Type of Article	Provided Function or Service	GDPR Article
	Security Review	*Article 32 – Security of processing (Ensure confidentiality, integrity and availability).* Ensure least privilege access; implement accountability via data owners; provide reports that policies and processes are in place and successful. *Article 34 – Communication of a personal data breach to the data subject.* *Article 35 – Data protection impact assessment (DPIA/Risk analysis).* Quantify regularly data protection risk profiles.
Accountability	Governance	*Article 37 – Designation of the data protection officer.* *Article 38 – Position of the data protection officer.* *Article 39 – Tasks of the data protection officer.*

4.6 Security and Privacy Implementation

4.6.1 Introduction

This section presents two use cases selected to illustrate the interest and the importance to follow a top-down approach for security and privacy. During the end-to-end security risk analysis and DPIA performed on the IoT systems of the ACTIVAGE project, this approach allowed the identification of the recommendations and solutions to put in place to improve the security of some IoT system components as well as the services/functions to cope with GDPR privacy requirements. It is clear that the Privacy services must run on top of a Secure IoT system.

The first use case presents the countermeasures implemented to secure the data storage of the Raspberry PI Gateway used in some Deployment sites of ACTIVAGE. The second use case presents several scenarios where the Blockchain technology can be used to provide efficient solutions on security and privacy for the ACTIVAGE's Deployment sites.

4.6.2 Securing a Gateway

The Gateway in an IoT device to Cloud architecture is a key element as it marks the frontier between the public and private domains. In this position

in the architecture, the Gateway is indeed both an entry path from inside to outside and reverse.

In a worst-case scenario, somebody gaining access to a Gateway gains access to other Gateways, by reproducing the attack at a massive scale. In the ACTIVAGE context, Gateways are often deployed in homes, and thus it is not possible to master the physical access to the hardware. Moreover, the Gateway, in a residential place, might be stolen more easily than a server in a data centre might be.

The Raspberry PI is a popular platform for its low cost, stability and good support. In experimental projects such as ACTIVAGE, it is the platform of choice to be used as a Gateway. The analysis done from ACTIVAGE questionnaires on IoT devices used in the 9 Deployment sites has shown that at least 4 out 9 deployment sites are considering using such hardware platforms as reference for their experiments.

However, the Risk analysis performed on the Raspberry PI has identified potential weaknesses regarding security. A major weakness concerns the SD Card mass storage. Due to its removable nature, this mass storage can be easily accessed from a third-party system by simply removing the SD Card and plugging it to a computer.

In this way, the content would be cleared and read/write operation unauthenticable making it easy for a hacker to read out and even replace sensitive information such as user's password, SSH private keys or other credentials that could enable privileged access to the entire system. Table 4.7 illustrates the impact assessment of the different stride attributes for the mass storage of the gateway in the ACTIVAGE context (deployment in residential homes). The initial DREAD rates on the third column shows potential impacts. The last column shows new rates while mitigating the risks with a secure element. A first counter-measure for this weakness would be to encrypt the entire SD Card, thus, it requires storing the encryption key in a safe place, which is readable by the processor and the firmware while booting the OS located on the storage. A common solution for such a safe storage is to use a Trusted Platform Module (TPM). TPMs are standardized electronic components which have security related functions such as random number, hash and key generators, encryption and decryption hardware engines and offers facilities to store in secure manner keys or sensitive data such as Platform Configuration Registers. These components are used for example for secured boot in UEFI bios. Table 4.7 shows on the two last right columns the new DREAD rate while using such a component, with highest risks reduce to a safer impact level.

Table 4.7 DREAD impact assessment

Threat Class	STRIDE Security Property	DREAD Rate	Mitigation Choices	Mitigation Technology	New DREAD Rate
T	Integrity(I)	2,2,2,1,2 => 1.8	Data storage shall be temper-resistant File system shall be adapted to the technology (read/write cycles) Data shall be backed up	Use a secure element to store security information in order to: Encrypt application's partition Manage strong authentication at network level and application level	2,2,2,1,2 => 1.8
R	Confidentiality(C)	2,2,2,1,2 => 1.8	Read and write operation shall require authentication		2,1,1,1,2 => 1.4
I	Confidentiality(C)	3,2,3,2,3 => 2.6	Data storage shall be encrypted		1,1,1,1,2 => 1.2
D	Availability(A)	2,2,2,1,2 => 1.8	Removable storage devices shall be proscribed Data storage resources shall be monitored to avoid being saturated		2,2,2,1,2 => 1.8
E	Authorization(I)	3,2,2,2,2 => 2.2	Write and Read permission shall be tuned in the file system		1,1,1,1,2 => 1.2

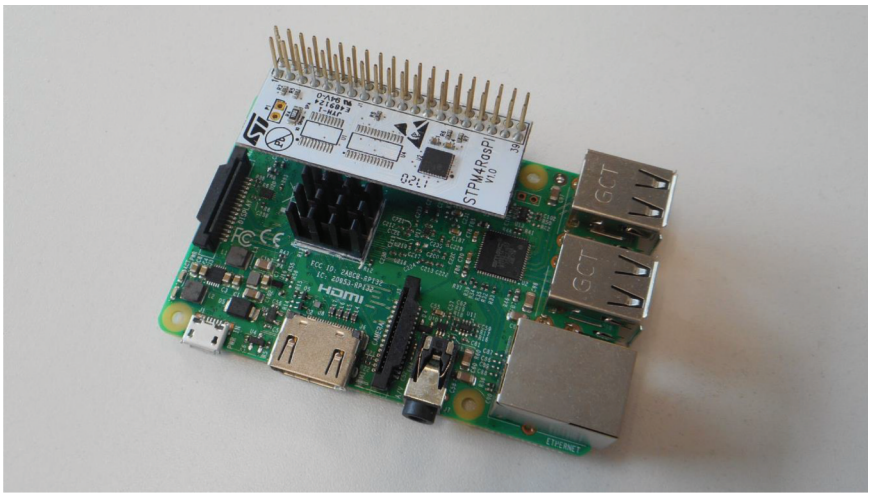

Figure 4.5 Raspberry PI model 3 with TPM dedicated hat in white.

Figure 4.5 shows a prototype hat for a Raspberry PI embedding a TPM manufactured and assembled in this form by STMicroelectronics. Customization of the Linux Kernel for enabling TPM support was also made with the appropriate device tree modification. The TPM is provisioned with security credentials bound to the ACTIVAGE Public key Infrastructure (PKI), ensuring security credential lifecycle up to the revocation of gateways that are suspected to be compromised. This PKI delivers certificates that can be used for the OS and application layer, with state-of-art cryptography scheme.

At the application level, ongoing work is focused on using the TPM secure function whenever possible. A first step consists in the partial encryption of the SD Card. Indeed, while the kernel is located on a clear partition for booting up, the application section is located into a LUKS partition which key is located onto the TPM. It prevents somebody reading the SD card from another platform. Future work will be to encrypt the entire SD card with the decryption within the boot loader.

Other work consists in emulating a PKCS11 interface from the TPM. PKCS11 is a standardized public key cryptography standard specifically related to tokens. The use of this standard enables trustful communication for the establishment of TLS or SSL tunnels, which can be used for the traffic between the Gateway and the Cloud. Use of such tunnels enables encrypted and authenticated communications and prevents the Gateway from being detectable on public network as no IP ports need to be opened for incoming

connections. Other use of this interface is under investigation for future work regarding IoT device provisioning.

4.6.3 Blockchain in Smart Homes

Recently, the Blockchain technology has been applied for the healthcare industry [26] but also in IoT-based Smart Homes [27], reducing the time required to access patient information, enhancing interoperability and improving data quality, while reducing maintenance costs. A Blockchain is a continuously growing list of immutable records, called blocks, which are linked and secured using cryptography. Thus, the adoption of Blockchain is a very promising technology towards enhancing the security, privacy and trust.

As described in the previous sections, ACTIVAGE gives special focus on GDPR compliance. Blockchain can act as a very useful tool towards achieving GDPR compliance [28], mainly by serving as a trusted decentralized repository for identification purposes. However, it has to be ensured that: a) no personal data are stored on the Blockchain, b) cryptographic data deletion should be used to give to the end-user the "right to be forgotten". Blockchain can also enhance security as it can enable IoT devices to connect securely and reliably avoiding the threats of device spoofing and impersonation. Every IoT device can be registered in the Blockchain and will have an ID that will uniquely identify this device in the universal namespace.

In the context of ACTIVAGE project, a trusted management solution, based on Blockchain technologies, has been proposed considering the results of other H2020 project implementations such as GHOST/H2020, myAirCoach/H2020. ACTIVAGE will find in this technology a convenient solution to cope with:

- Privacy regulation based on GDPR.
- The integrated healthcare and AHA implications for data and devices protection.
- An adequate trusted mechanism for IoT-based devices, users and systems within the smart Home environment.

The concept of distributed ledger technologies can be introduced within ACTIVAGE to support different use case scenarios such as:

- Requesting/giving/updating permissions for accessing personal data of the involved user.
- Device registration.
- Timely firmware updates.

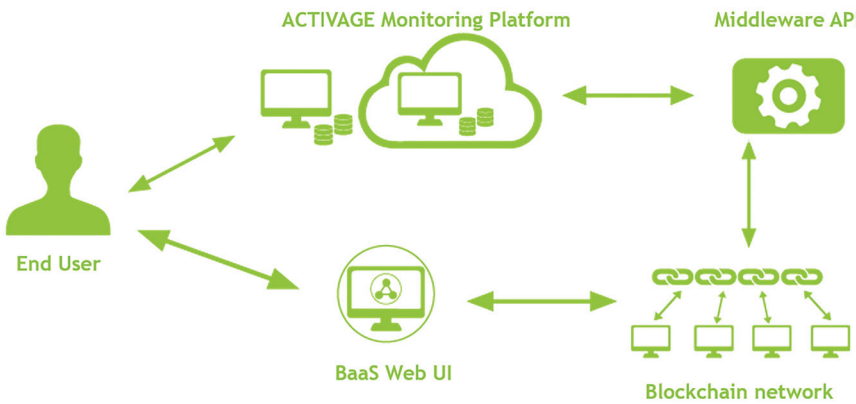

Figure 4.6 ACTIVAGE monitoring platform – BaaS platform architectural overview.

- User authentication & authorization.
- The secure data transfer between endpoints, users and healthcare network components.

Towards the formulation of a secure and trusted environment using information traceability mechanisms and the spreading of the data in AHA information systems, a related ACTIVAGE Blockchain framework has been introduced (see Figure 4.6) consisting of the following main components:

- **BaaS Web UI** (The Blockchain-as-a-Service (BaaS) Web UI) – It is a web front-end for accessing the functionalities provided by the Blockchain network that has been implemented within myAirCoach H2020 project.
- **Middleware API** – The Middleware API enables the communication between the ACTIVAGE Monitoring Platform and the Blockchain network. For this purpose, RESTful web services are used over the HTTPS protocol.
- **Blockchain network** – This is the network of Blockchain nodes where information regarding the various transactions are being stored.
- **ACTIVAGE decentralised Monitoring Platform** – This is a decentralised platform where raw data gathered from the sensors installed in the smart homes of the elderly users are stored and further analysed towards identifying patterns related to user activity (e.g. habits, sleeping times, etc.) and further identifying abnormal events that may be related to emergencies. Through the ACTIVAGE Monitoring Platform and all the other Blockchain components, a trusted environment is offered to the formal/informal carers/end-users as well as to the elderly users/patients.

In the following paragraphs, several use case scenarios for using Blockchain technology within ACTIVAGE are described.

4.6.3.1 Register in BaaS/give consent

In this scenario, the user accesses the registration form in the BaaS Web UI by clicking on the relevant link. After filling the registration form with their data and accepting the Terms of Service, a verification email is sent to their email address. By clicking on the hyperlink, included in the corresponding email, the user is redirected to the BaaS Web UI and their email is verified. After the email verification process, the user can Login the BaaS Web UI. The transaction related to user registration is logged in the Blockchain.

4.6.3.2 Register in the ACTIVAGE monitoring platform through BaaS

A user is able to register to the ACTIVAGE Monitoring Platform from the BaaS Web UI. Thus, the user first logs in to BaaS with his/her account, goes to "Platforms > Not Registered Platforms", chooses ACTIVAGE from the list and clicks on the "Register" button. Then, user is redirected to the ACTIVAGE Monitoring Platform and fills in the Registration Form. Similarly, to the previous scenario, an email verification process is followed for the completion of user registration in the ACTIVAGE Monitoring Platform. The next time that the user logs in the BaaS Web UI, ACTIVAGE is among his/her "Registered Platforms". Again, the transaction related to user registration is logged in the Blockchain.

4.6.3.3 Register in the ACTIVAGE monitoring platform with BaaS

In this scenario, user fills in the Registration Form in the ACTIVAGE Monitoring Platform (option: Register via BaaS). The ACTIVAGE Monitoring Platform sends the valid credentials of the user to the Middleware API through a RESTful Web Service. Then, the Middleware API sends the registration request to the user via email and redirects them to the BaaS Web UI Registration Form. The user registers using the BaaS Registration Form and this transaction of the newly Registered User is logged in the Blockchain network.

4.6.3.4 Registration of new devices and software updates

In ACTIVAGE, Blockchain can be applied not only for the secured registration and authorization of users, but also for the envisaged IoT-based devices that are being installed in the smart Home environment supporting also the timely update of firmware, patches, etc., in order to be performed only by authorized users.

4.6.3.5 Login/Logout

When the user logs in/out to/from the ACTIVAGE Monitoring Platform, a corresponding request for user login/logout is automatically sent to the middleware API over a RESTful Web Service. The Middleware API updates the list with online Users that are kept within the Blockchain by adding/removing the User to/from the list. Thus, all login/logout processes are logged in the Blockchain network.

4.6.3.6 Request/Give/Update permissions for accessing personal data

In this scenario, depicted in Figure 4.7, a caregiver asks for permission to access the personal data of an elderly person through the ACTIVAGE monitoring platform. This request is sent to the Middleware API, which logs it in the Blockchain by also sending a request for permission approval to

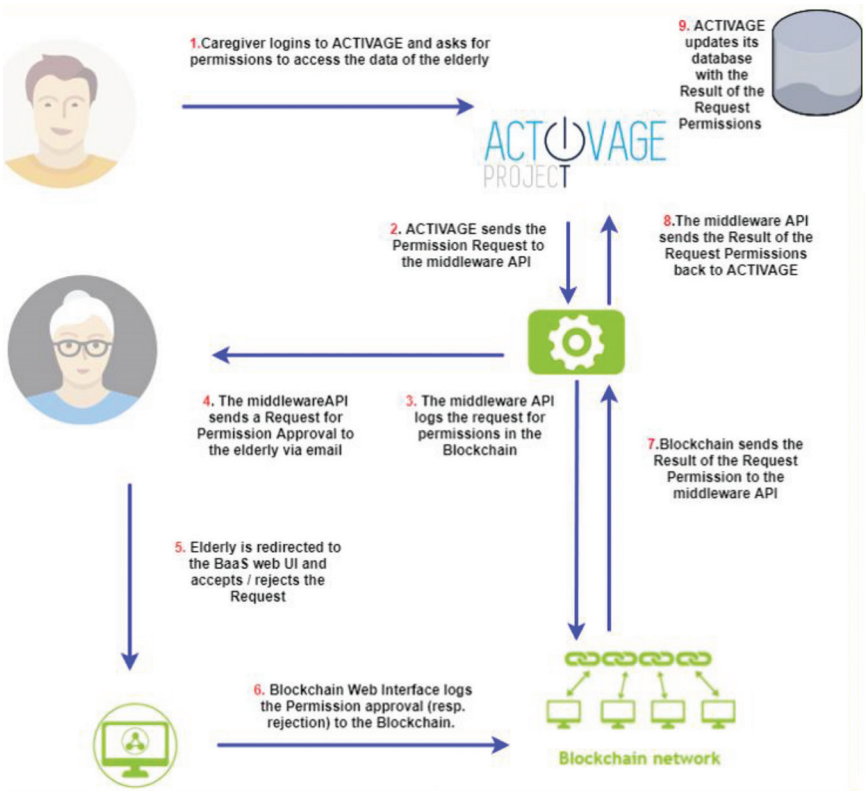

Figure 4.7 Request permissions for accessing personal data.

the elderly via email. By using the hyperlinks included in the email, the elderly is directed to the BaaS Web UI where he/she can accept or reject the request and the corresponding approval/rejection is also logged in the Blockchain network. Through the Middleware API, the result is sent back to the ACTIVAGE Monitoring Platform and based on the decision of the elderly the caregiver is able or unable to access the personal data of the elderly.

These scenarios give a good overview of the possibilities offered using Blockchain technology in AHA applications and more particularly its implementation and validation through the ACTIVAGE project in order to ensure security and privacy in its deployment sites.

4.7 Conclusions

In this chapter, two complementary methodologies were presented one for security and the other for privacy in order to address the challenges presented in the previous paragraphs. They were developed to help the IoT System developers of ACTIVAGE to secure their systems and implement correctly personal data protection to cope with the GDPR requirements. These methodologies follow a twofold approach a top down and an end-to-end. These approaches concern from one side the security risk analysis to identify in advance potential threats and find the countermeasures to mitigate/avoid them. From the other side, a privacy approach to put in place the GDPR following a DPIA analysis to identify the system characteristics and evaluate the risks related to the personal data and its protection. This work, developed in the frame of the ACTIVAGE project, can be also reused for any other IoT system considering the high constrains on security and privacy required by AHA applications.

Finally, the solutions presented give a good overview of the possibilities offered by the use of the Secure element component to secure IoT devices (Gateways and Sensor nodes) and the Blockchain technology in AHA applications. Both technologies will take an important place in the implementation and validation of the security and privacy requirements of the ACTIVAGE's Deployment sites to provide secure IoT systems with a high level of personal data protection and thus to increase the users' trust.

Future work will put in place and validate these methodologies and the potentials solutions to secure the 9 Deployment sites of ACTIVAGE project as well as the protection of the personal data of each of the seven thousands of patients "elderly people" participating in the project.

Acknowledgement

This research project has received funding from the European Union's Horizon 2020 research and innovation programme ACTIVAGE under grant agreement N° 732679.

The activities concerning the Secure Gateway has received funding from the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-10-AIRT-05)".

References

[1] Internet Security Threat Report ISTR Ramsonware 2017 An ISTR Special Report July 2017.

[2] Proposal for a Regulation OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification "Cybersecurity act"), online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505290611859&uri=COM:2017:477:FIN

[3] Internet of Things European Large-Scale Pilots Programme, online at: https://european-iot-pilots.eu

[4] ACTIVAGE Large-Scale Pilot project, online at: https://www.activage project.eu/

[5] General Data Protection Regulation (GDPR) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Official journal of the European Union, online at: https://gdpr-info.eu/

[6] NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004), online at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[7] NIST SP 800-53A, NIST Special Publication 800-53A. Revision 4. Assessing Security and Privacy. Controls in Federal Information. Systems and Organizations (December 2014), online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

[8] Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung, The Internet of Things: New Interoperability, Management and Security Challenges

International Journal of Network Security & Its Applications (IJNSA) Vol. 8, No. 2, March 2016.

[9] Managing security recommendations in Microsoft Azure Security Center, online at: https://docs.microsoft.com/en-us/azure/security-center/security center-recommendations

[10] Baseline Security Recommendations for IoT - Interactive tool, European Union Agency for Network and Information Security, online at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security-recommendations-for-iot-interactive-tool

[11] CERN Computer Security Recommendations, in CERN Computer Security, online at: https://security.web.cern.ch/security/recommendations/en/index.shtml

[12] Security Recommendations to Prevent Cyber Intrusions, US-CERT, Official website of the Department of Homeland Security, on line at, https://www.us-cert.gov/ncas/alerts/TA11-200A

[13] Privacy and Data protection by Design ENISA, Retrieved 2017 04-04, online at: https://www.enisa.europa.eu

[14] Ann Cavoukien, Privacy by Design, The 7 foundational Principles Information & Privacy Commissioner Ontario, Canada Originally Published: August 2009, Revised: January 2011.

[15] IoT Security Compliance Framework, Release 1.0 2016, IoT Security Foundation

[16] IoT Trust Framework, v2.0 – Released Jan 5, 2017, OTA (Online Trust Framework)

[17] Top 10 IoT security issue categories, OWASP proposal.

[18] Stride THREAT Modelling developed by Microsoft: https://msdn.microsoft.com/enus/library/ee823878%28v=cs.20%29.aspx, https://fr.slideshare.net/marcomorana/application-threat-modeling-presentation, http://www.cs.berkeley.edu/~daw/teaching/cs261f12/hws/IntroductiontoThreatModeling.pdf, http://resist.isti.cnr.it/freeslides/security/williams/RiskBasedSecurityTesting.pdf, https://users.encs.concordia.ca/~clark/courses/1601-6150/scribe/L04c.pdf

[19] Ronen, A. Shamir, A. O. Weingarten and C. O'Flynn, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 195–212. doi: 10.1109/SP.2017.14

[20] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679; Adopted on 4 April 2017.

[21] Recommendations for a privacy impact assessment framework for the European Union, Deliverable D, online at: http://www.piafproject.eu/ref/PIAF D3 final.pdf
[22] RFID PIA Tool: GS1 EPC/RFID Privacy Impact Assessment Tool, online at: http://www.gs1.org/pia
[23] Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, Smart Grid Task Force 2012–14, March 18th, 2014.
[24] Mario Diaz Nava and al., "Report on IoT Devices" Deliverable 3.6 of ACTIVAGE/H2020/LSP, March 2018.
[25] GDPR A practical Guide, Varonis.
[26] Blockchain: A healthcare Industry view, online at: https://www.capgemini.com/wp-content/uploads/2017/07/blockchain-a healthcare industry view 2017 web.pdf
[27] Ali Dorri, Salil S. Kanhere, and Raja Jurdak, Blockchain in Internet of Things: Challenges and Solutions: A healthcare Industry view, online at: https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf
[28] Grant Thornton, GDPR & blockchain – Blockchain solution to General Data Protection Regulation, online at: https://www.grantthornton.global/globalassets/_spain_/links-ciegos/otros/gdpr--blockchain.pdf