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

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D5.5: ARCADIAN-IoT Use Cases Validation and Legal Compliance – Final Version

Revision: v.1.0

Work package	WP 5
Task	Task 5.5
Due date	30/04/2024
Submission date	22/05/2024
Deliverable lead	IPN
Version	1.0
Partner(s) / Author(s)	IPN: Fernando Bastos, Paulo Silva, Rúben Leal, Sérgio Figueiredo UWS: Jose M. Alcaraz Calero, Qi Wang, Antonio Matencio Escolar, Ignacio Martinez-Alpiste, Pablo Benlloch Caballero, Julio Diez-Tomillo 1GLOBAL: João Casal, Afonso Paredes, Ivo Vilas Boas XLAB: Nejc Bat, Klemen Kobau MARTEL: Andrea Falconi, Gabriele Cerfoglio, Giacomo Inches BOX2M: Alexandru Gliga, Ovidiu Diaconescu, Marian Macoveanu RISE: Alfonso Iacovazzi, Han Wang ATOS: Ross Little RGB: Ricardo Ruiz LOAD: Pedro Colarejo E-LEX: Adriana Peduto, Elisa Cristina, Fabiola Iraci UC: Bruno Sousa, Luís Paquete, João Nunes

Abstract

This public report constitutes the deliverable D5.5 of ARCADIAN-IoT, a Horizon 2020 project with the **grant agreement number 101020259**, under the topic **SU-DS02-2020**. The main purpose of the report is to describe ARCADIAN-IoT use cases implementation, validation and the framework's evaluation enabled by the final Prototype P2.

The material presented in this document is the main outcome of **Task 5.5,** final version for P2, **(ARCADIAN-IoT Use Case Technical and Legal Compliance Validation)** and has considered inputs from Task 2.2 (Architecture & Use Cases); Task 5.1 (Integration of ARCADIAN Framework); Tasks 5.2 to 5.4 (Use Case implementations for the ARCADIAN-IoT Domains A, B and C); and as outputs for T5.6 (Training material). Therefore, the following deliverables have been used as the input and the base for this deliverable: D2.2 [1, which specified the initial high level use cases; D2.5 [2] and D5.2 [5], which specified and revised the architecture, respectively; D5.3 [3] and D5.4 [4] which described the use case implementations and ARCADIAN-IoT's validation in the first prototype (P1). respectively. Furthermore, the ethical considerations raised in D7.6 [10] have served as input to the document, especially concerning the collection and handling of personal data, including sensitive data in the domains.

All technical partners have been involved in the iterative process of specification, implementation, validation and evaluation of the ARCADIAN-IoT Framework.

Keywords:

ARCADIAN-IoT Framework; Use cases Implementation, Technical and Legal Validation, Framework KPI evaluation

Document Revision History

Version	Description of change	List of contributors
V0.1	ToC and initial definition of contents	IPN
V0.2	First draft with section filling instructions	IPN
V0.3	Filling technical sections for validation scenarios and results	IPN, LOAD, 1GLOBAL, ATOS, RGB, UWS, XLAB, RISE
V0.4	Merge of scenario description with results and addition of P2 use case stories	IPN, LOAD, 1GLOBAL, ATOS, RGB, UWS, XLAB, RISE, MARTEL, BOX2M, E-LEX, UC
V0.5	Partial inclusion of validation scenarios results and objectives; Added executive summary	IPN, LOAD, 1GLOBAL, ATOS, RGB, UWS, XLAB, RISE, MARTEL, BOX2M, E-LEX, UC
V0.6	Expert review (sections 1-3)	UWS
V0.7	Modifications according to Expert review	All partners
V0.8	Expert review (sections 4-7)	UWS
V1.0	Final review before submission	IPN

Disclaimer

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	

EXECUTIVE SUMMARY

ARCADIAN-IoT framework proposes an integrated approach for managing identity, trust, privacy, security and recovery, across IoT devices, persons and services, relying on specialized components distributed across Vertical and Horizontal planes. The vertical planes cover Identity, Trust and Recover management, while the horizontal planes oversee the management of privacy and security across the framework.
This document - Deliverable 5.5 (ARCADIAN-IoT Use Cases Validation and Legal Compliance – Final version) - describes the ARCADIAN-IoT validation specifications and execution activities for the 3 Domain Use Cases performed for the **final prototype - P2**. It starts by restating ARCADIAN-IoT's conceptual architecture, with emphasis on the collective contribution of each of its planes, as well as the IoT application domains and the performed integration approach. It then reviews the use cases – defined in the context of the referred IoT application domains - which have served for guiding the P2 validation activities, also presented herein. The evaluation of the ARCADIAN-IoT framework – both through its project-wide and component-specific KPIs – are then presented and justified in relation to the validation use cases. Taking into account the presence of legal compliance risks derived from the development or interaction with the scoped technologies (e.g. biometrics, AI, health data processing), the related analysis is equally provided.

The material presented in this document is the main outcome of **Task 5.5 (ARCADIAN-IoT Use Cases Validation and Legal Compliance)** and builds both on the requirements, architecture and use cases specifications (resulting from WP2), the research and implementation of each ARCADIAN-IoT component (addressed in WP3 and WP4), the integration of the ARCADIAN-IoT Framework (scoped in T5.1) and the preparation and implementation of the use cases (Tasks 5.2, 5.3 and 5.4).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3PP	3rd Party Platform
ABE	Attribute Based Encryption
AI	Artificial Intelligence
AIDS	Anomaly Intrusion Detection System
aiotID	ARCADIAN-IoT ID
BLE	Bluetooth Low Energy
CoT	Chain of Trust
CTI	Cyber Threat Intelligence
DB	Database
DGA	Drone Guard Angel
DID	Decentralized Identifiers
DIW	Digital Identity Wallet
DLT	Distributed Ledger Technologies
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
EU	European Union
FE	Functional Encryption
FL	Federated Learning
GMS	Grid Management Service
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile communications Association
HE	Hardened Encryption
HIDS	Host Intrusion Detection Systems
ICS	Industrial Control Systems
IdP	Identity Provider
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoC	Indicator of Compromise
IoT	Internet of Things
IPR	Intellectual Property Rights
IT	Information Technologies
KPI	Key Performance Indicator
LTE	Long Term Evolution
LTE-M	Long Term Evolution, category M1
NBAE	Network-Based Authorization Enforcement
NBIoT	Narrowband Internet of Things
NMAP	Network Mapper
OTA	Over-the-Air
OWASP	Open Web Application Security Project
PCA	Protection Control Agent
PII	Personally Identifiable Information
R&I	Research & Innovation
RATS	Remote Attestation Procedures
RIA	Resource Inventory Agent
RoT	Root of Trust

RSP	Remote SIM Provisioning
SE	Secure Element
SHDM	Self-Healing Decision Manager
SIDS	Signature Intrusion Detection System
SIM	Subscriber Identification Module
TCP	Transmission Control Protocol
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
VDR	Verifiable Data Registry
W3C	World Wide Web Consortium
WP29	Article 29 Data Protection Working Party

1. INTRODUCTION

This section starts by laying the objectives and assumptions for this deliverable, such as its relationship with ARCADIAN-IoT's final prototype (P2). It is followed by a presentation of key background information pertaining to P2 (i.e., target IoT application domains, validation and evaluation methodology). The section concludes with a presentation of the overall document structure and organization.

1.1 Objectives and Assumptions

The main purpose of this report is to document the **validation activities and results of the final prototype (P2)** of ARCADIAN-IoT framework. P2 was documented in Deliverable D5.2 (Integration of ARCADIAN-IoT framework) [1] and provided a final version of ARCADIAN-IoT functionalities building on the integration of the different architectural planes and respective components. The validation activities are performed in the context of different IoT application domains for which a series of use cases was established. Thus, it depends on the availability of the different use cases artifacts (e.g., service-specific software or hardware) which have been produced or adapted by the IoT service providers / use case owners (in the scope of Tasks 5.2, Task 5.3 and Task 5.4) for leveraging ARCADIAN-IoT framework. The validation activities have also served the purpose of supporting the evaluation of ARCADIAN-IoT framework, with such evaluation consisting of two sets of KPIs:

- The project-wide KPIs, which have been defined at proposal stage and which are linked to specific Objectives of the project;
- The specific KPIs identified for each component of the ARCADIAN-IoT framework - belonging to the Horizontal and Vertical planes (WP3 and WP4, respectively) - which have been defined during the project execution.

It is noted that the prototyping activities (i.e. both initial P1 and final P2) have contributed with significant knowledge which was leveraged for performing the training activities targeting the different relevant ICT and non-ICT stakeholders (scoped in Task 5.6).

1.2 Validation Background

This deliverable builds upon several different inputs from multiple Work Packages. First and foremost, from WP5 it leverages the prototyping of ARCADIAN-IoT (P1 and P2, documented in D5.1 and D5.2, respectively) performed within T5.1 scope. P1 and P2 prototypes have been guided by the initial use cases specifications (D2.2) and subsequent revisions undertaken as part of T5.2, T5.3 and T5.4 for Domain A, B and C, respectively: the first revision was performed in D5.3 for P1 and the final revision has been performed for P2 and included in the present document. The idealistic, comprehensive use case specifications serve as core information for establishing pragmatic and more focused validation scenarios.

Moreover, from WP3/WP4, adding to the Horizontal/Vertical planes functionalities provided for supporting the prototype(s), component specific KPIs have been established, providing concrete evaluation targets.

To ensure the success of the validation activities, which require functional prototypes of the technical components, there was a considerable effort in establishing the target scenarios set for the final version of the ARCADIAN-IoT framework (P2).

1.3 Document Structure

The remainder of this document is presented as follows:

Section 2 details the architectural environment used for the validation and evaluation activities, including all the integrated Framework Components (Horizontal and Vertical). It also provides an overview of all the scoped use cases and the main security roles played by the components.

Section 3 Provides a detailed and revised description of each of the use cases and the implementation activities.

Section 4 Presents the specified validation scenarios, including the involved ARCADIAN-IoT components and the scenarios implemented. It also includes validation achievements and results, performed during T5.5 validation activities.

Section 5 Describes the evaluation KPIs associated to the different ARCADIAN-IoT components, and which provide targets for P2 evaluation. Provides evaluation results and also analyses the current achievements with respect to the overall ARCADIAN-IoT project objectives and KPIs.

Section 6 Is responsible for the specification of the Legal compliance validation activity addressed for the P2 Prototype.

Section 7 Summarizes the main points and achievements of the Task T5.5, namely for the validation and evaluation results of P2 prototype.

2. OVERALL ARCHITECTURE AND USE CASE OVERVIEW

2.1 Conceptual Architecture

As outlined in the ARCADIAN-IoT Grant Agreement [6], the project aims to develop a cyber security framework relying on a novel approach to manage and coordinate, in an integrated way, identity, trust, privacy, security, and recovery in IoT systems. The proposed approach organizes the multiple cyber security functionalities offered by the framework into several planes combined in an optimized way to support the end-to-end services. In particular, the framework includes three Vertical Planes devoted to identity, trust, and recovery management, and three Horizontal Planes supporting the Vertical Planes by managing privacy of data, monitoring security of entities, and providing Permissioned Blockchain and Hardened Encryption technologies (see Figure 1).

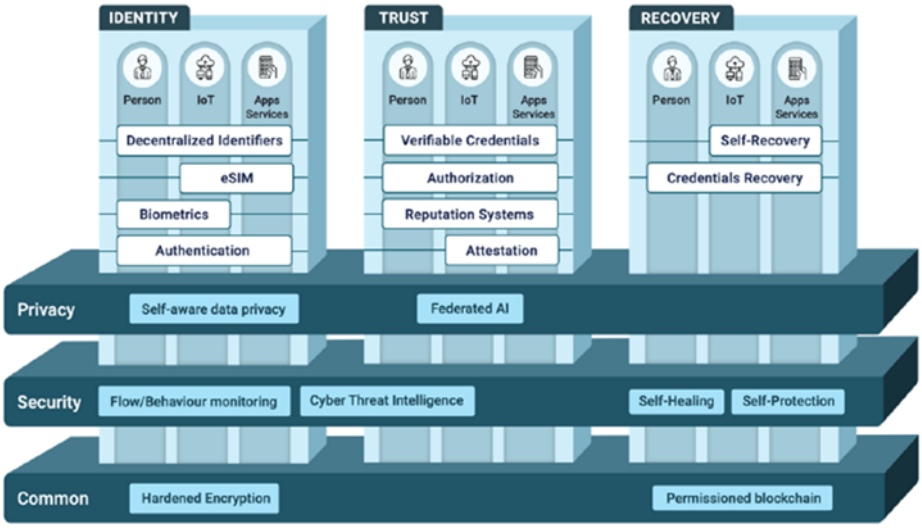

Figure 1 - ARCADIAN-IoT framework [6]

Deliverables D3.3 [7] and D4.3 [8] describe in detail the Horizontal and Vertical Planes (respectively) and the components identified and developed in each plane. D5.2 [5] describes the involvement of the different ARCADIAN-IoT components in each use case.

The following subsections provide a compact view of the various planes of ARCADIAN-IoT (for a detailed analysis please refer to D5.2). To support this goal, figures depicting both inner- and inter-plane views (i.e. for dependencies or interactions with components from other planes) are provided – refer to the associated captions shown in Figure 2.

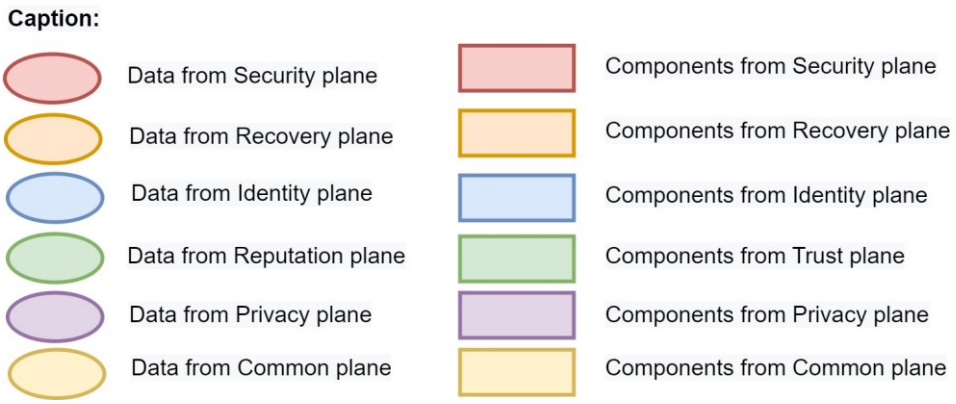

Figure 2 - Captions for plane-centric representations

2.1.1 Privacy Plane

The privacy plane aims to provide functionalities for the privacy-preserving management of confidential or sensitive data involving persons' entities and is constituted by Federated AI and Self-Aware Data Privacy. As shown in Figure 3, Federated AI supports the decentralized properties of the Security Plane (i.e. Device Behaviour Monitoring (DBM) and Cyber Threat Intelligence (CTI)), while Self-Aware Data Privacy interacts with Hardened Encryption and Authentication for enabling its role in the establishment of encryption and decryption access policies.

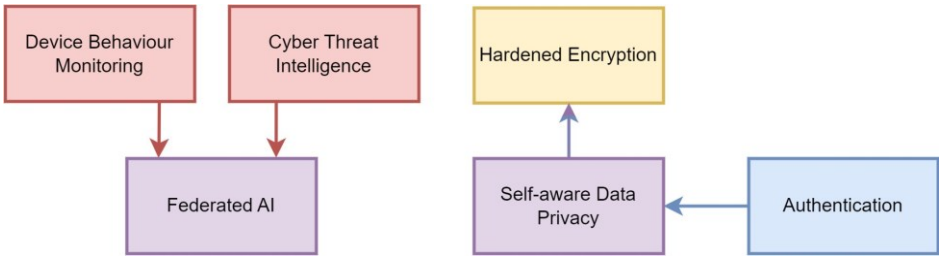

Figure 3 – Key ARCADIAN-IoT interactions from the point of view of Privacy Plane

2.1.2 Security Plane

The security plane provides cyber security features required for the monitoring, prevention, protection and healing against incidents in IoT devices or network. Six components form the security plane: Cyber Threat Intelligence, Device Behaviour Monitoring, Device Self-Protection, Network Self-Healing, Network Self-Protection, and Network Flow Monitor. As shown in Figure 4, besides the communications internal to the plane (e.g., intrusion events from device and network segments towards CTI, network self-healing and self-protection), the security plane has key interactions with other planes such as Trust (e.g., transmission of IoCs towards Reputation System, consumption of reputation updates) or Privacy (where Federated AI has a key role in both DBM and CTI).

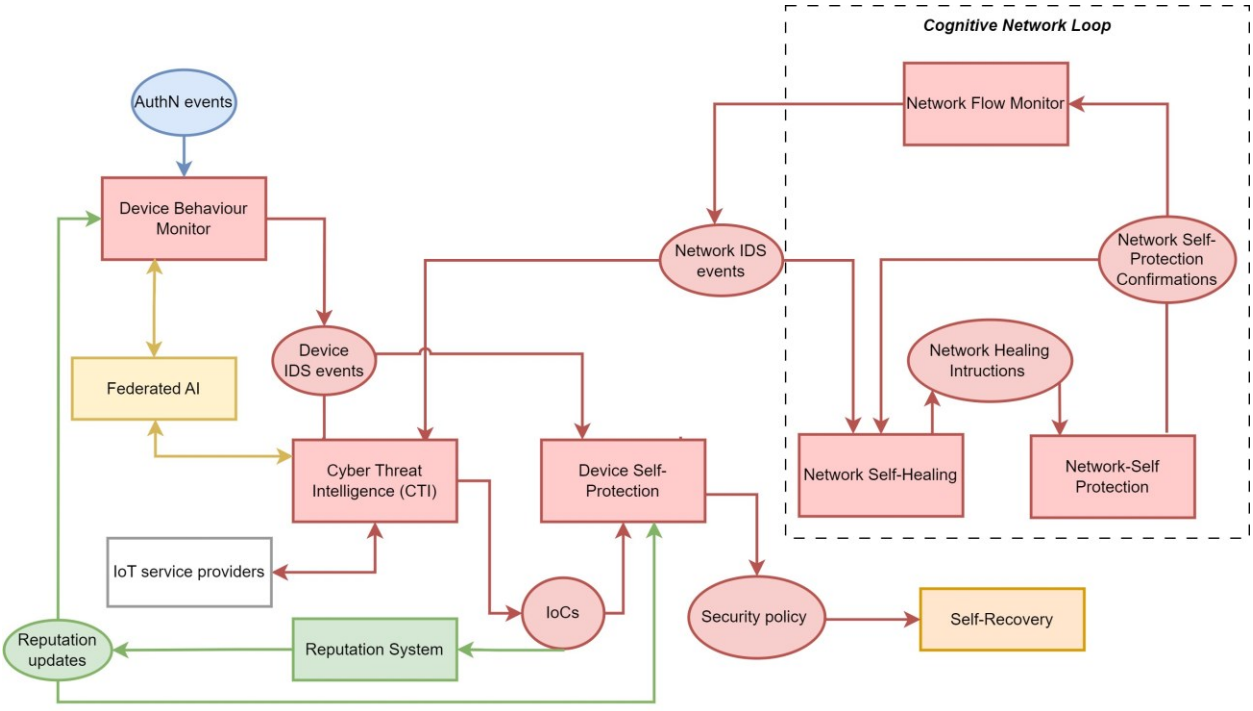

Figure 4 - Key ARCADIAN-IoT interactions from the point of view of Security Plane

2.1.3 Identity Plane

The Identity Plane enables the management of identities of the different entities (e.g., persons, devices and ARCADIAN-IoT components), and comprises multiple identification schemes. Five components constitute the identity plane: Decentralized Identifiers, Authentication, SIM[1], Network Credentials and Biometrics. As shown in Figure 5, they not only interact among themselves but also with components from the common plane (Blockchain and Hardened Encryption), trust plane and privacy plane. The shared information considers, among others, communication payload requiring encryption, authentication events or identification results.

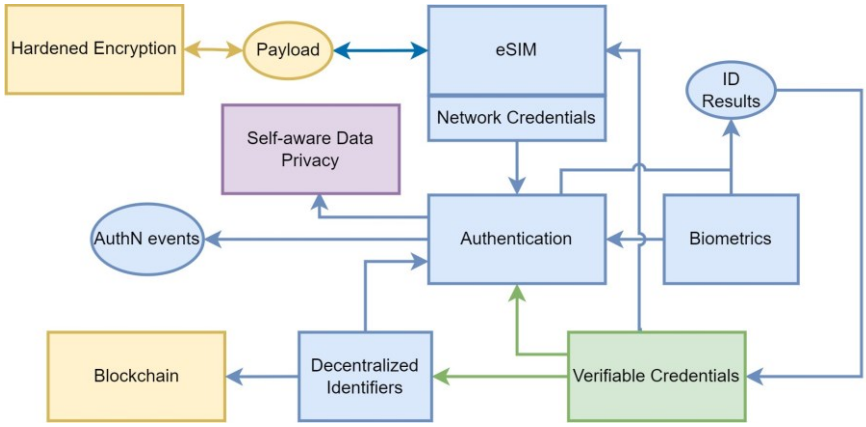

Figure 5 – Key ARCADIAN-IoT interactions from the point of view of Identity Plane

2.1.4 Trust Plane

The Trust plane implements mechanisms for managing trust on the involved entities (persons, devices and services). The four components which constitute it are Remote Attestation, Reputation System and (Network) Authorisation and Verifiable Credentials. As shown in Figure 6, they interact with components from all the other planes. This is especially evident due to the role of the reputation system on the framework. The shared information considers, among others, reputation events and reputation score updates, attestation results, Indicators of Compromise or identification results.

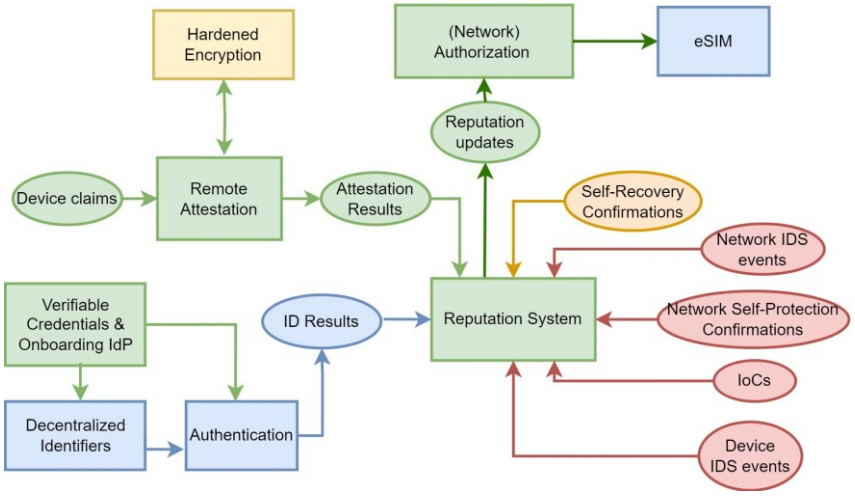

Figure 6 - Key ARCADIAN-IoT interactions from the point of view of Trust Plane

[1] The technology built (e.g., SIM applets) apply to any SIM form factor (SIM, eSIM or iSIM)

2.1.5 Recovery Plane

The Recovery plane addresses recovery management of data associated to the different types of entities, with two components forming it: Self-Recovery and Credentials Recovery. As shown in Figure 7, they interact with components from all the other planes. The shared information considers, among others, the information to the initiation of data or service recovery or confirmations of device self-recovery actions.

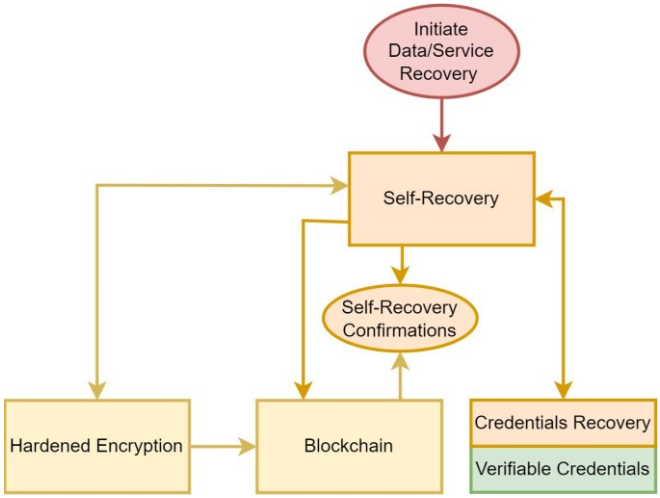

Figure 7 – Key ARCADIAN-IoT interactions from the point of view of Recovery Plane

2.1.6 Common Plane

The Common Plane includes two components that, as depicted in the previous planes, provide common functionalities which are leveraged by the Vertical Planes: Hardened Encryption and Permissioned Blockchain.

2.2 ARCADIAN-IoT Overall deployment view

The deployment view of ARCADIAN-IoT across the different locations or segments, from D5.2 [5], is recapped below.

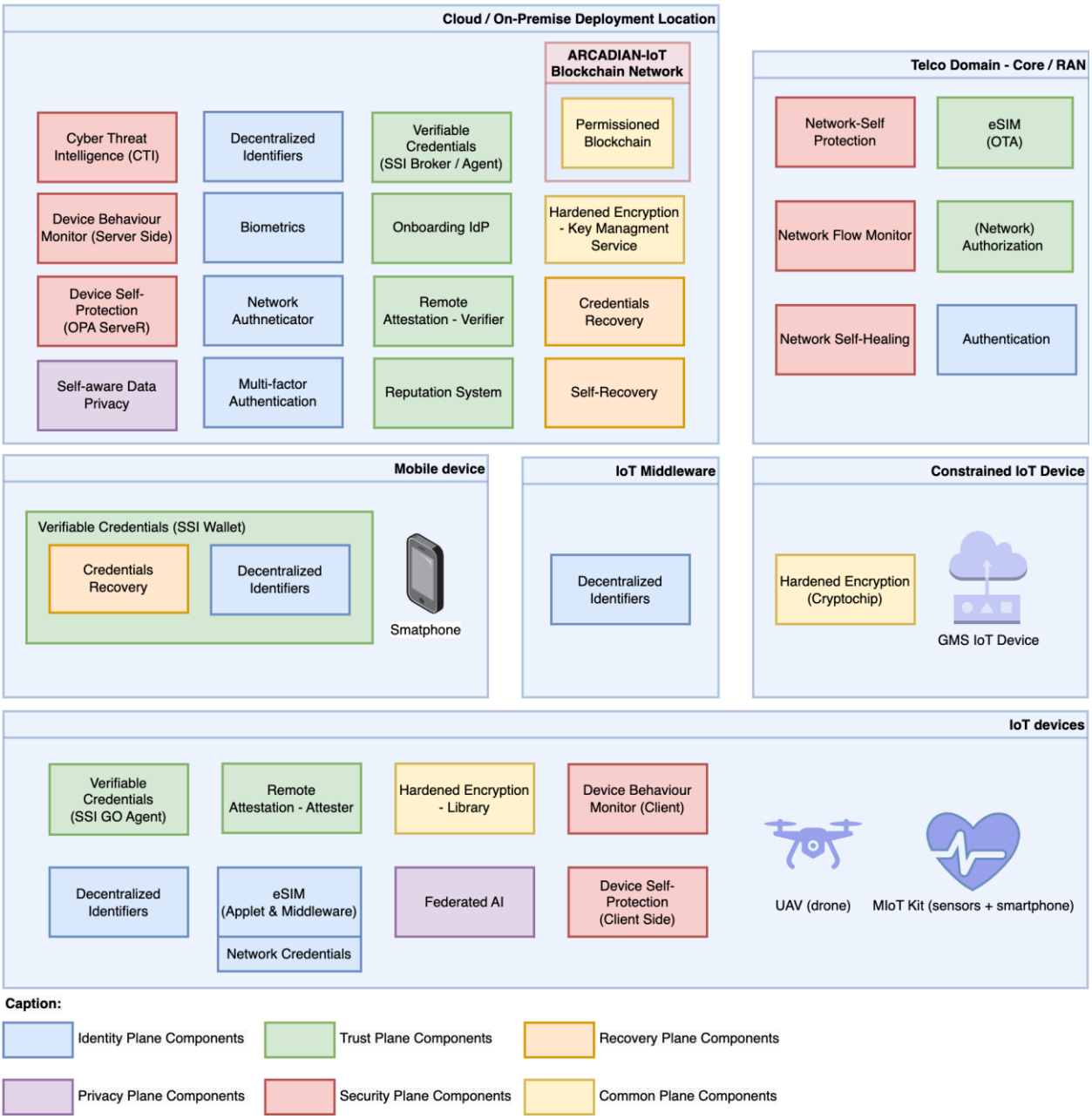

Figure 8 - ARCADIAN-IoT deployment view [5]

2.3 Use cases overview

The following subsections provide an overview of the 1) use cases of each domain, and 2) mapping of component integration in each use case.

2.3.1 Domain and Use Case Mapping

The use cases in scope of the project and included for the final validation are recapped in the following table, sub-divided by Domain, and identified according to the prototype where they were first supported (P1 or P2). Use cases at least partially supported in P1 are represented with blue background, while use cases supported in P2 appear with green background.

Table 1 - List of use cases targeted for ARCADIAN-IoT support

Domain	Use case ID	Use case name
Domain A – Emergency and Vigilance Using Drones and IoT	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
Doman B – Grid Infrastructure Monitoring	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
Domain C – Medical IoT	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	Monitor a patient and update a patient monitoring protocol
	C5	Patient MIoT devices security or privacy incident
	C6	MIoT Cloud services security or privacy incident
	C7	Medical 3rd party security or privacy incident

The detailed specification of each use case is presented in Section 3.

2.3.2 Use cases and components mapping

Each of the use cases has different Identity, Privacy, Trust, Security or Recovery requirements depending on its scope (as defined per D2.2). Consequently, the subset of ARCADIAN-IoT functionalities / components involved in each use case varies accordingly. The next figure depicts ARCADIAN-IoT involvement in each use case, namely, green boxes demark components which have been integrated in the use case (while grey boxes demark their absence).

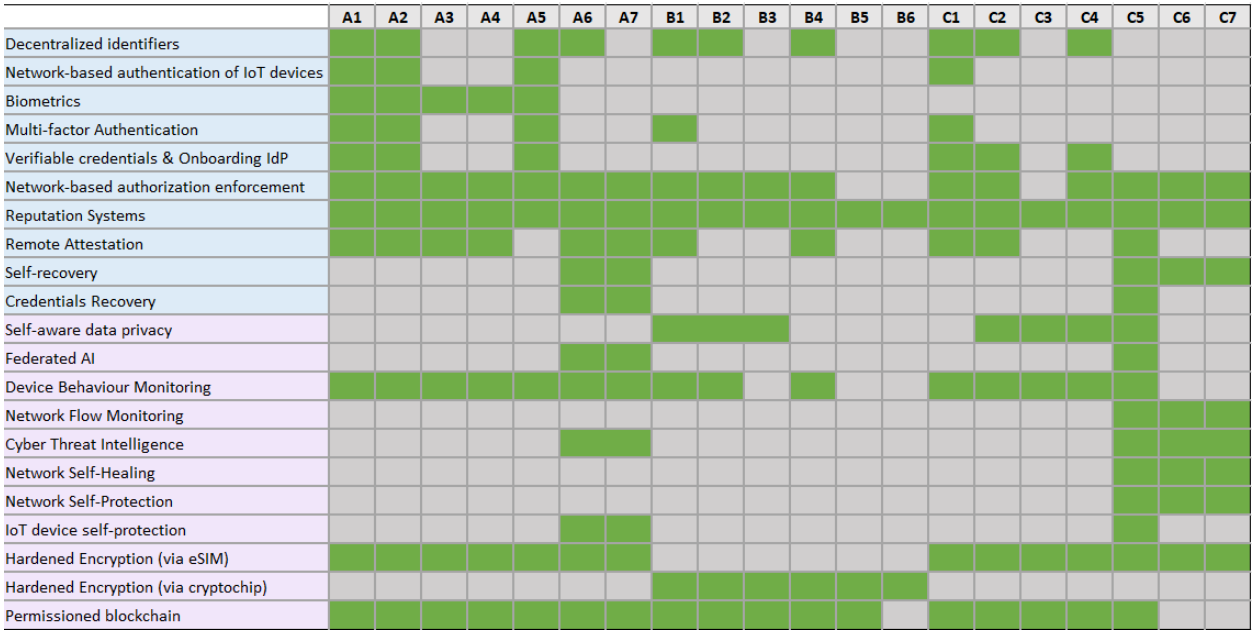

Figure 9 - Overview of ARCADIAN-IoT integration per use case (from D5.2 [1])[2]

[2] Hardened Encryption (via eSIM) was wrongly missing from use case A1 in D5.2, even though its integration description was provided.

3. USE CASES DESCRIPTION AND IMPLEMENTATION

This section provides an overall description of the use cases and their implementation across the three ARCADIAN-IoT pilot domains:

- Domain A: Emergency and vigilance using drones and IoT, which addresses a Drone Guard Angel (DGA) service, that enables drones to track and follow persons walking from one place to another, on their daily activities, in city areas.
- Domain B: Grid Infrastructure Monitoring, which addresses a secure and efficient solution for monitoring main grid circuits of industrial and public (e.g. smart cities) infrastructures.
- Domain C: Medical IoT, which addresses the monitoring and follow-up of cancer patients in the active treatment process.

In each domain, the application domain context is initially described. Each use case is then characterized using the following structure or template:

i) **Overview**: a short overview of the functionality demonstrated in the use case.
ii) **Use case description**: the detailed use case description, reviewing the high-level description initially provided in D2.2, including preconditions and postconditions, and main data flow.
iii) **Implementation details**: describes the pursued activities from the IoT service provider (domain owner) point of view in order to integrate ARCADIAN-IoT Identity, Security, Trust, Privacy and Recovery-related features required enabling the use case.

3.1 DOMAIN A – Emergency and vigilance using drones and IoT

3.1.1 Application domain context

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 centres). ARCADIAN-IoT domain A focuses on the use of IoT devices, in this case, drones, in novel efficient and citizen-centred urban vigilance services (Figure 10).

Illustrating a potential story of this IoT solution, high-level scenarios can feature a woman, Ana, who is on her way home alone, after a dinner with friends. Using ARCADIAN-IoT Drone Guard Angel (DGA) app in her personal smartphone 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.

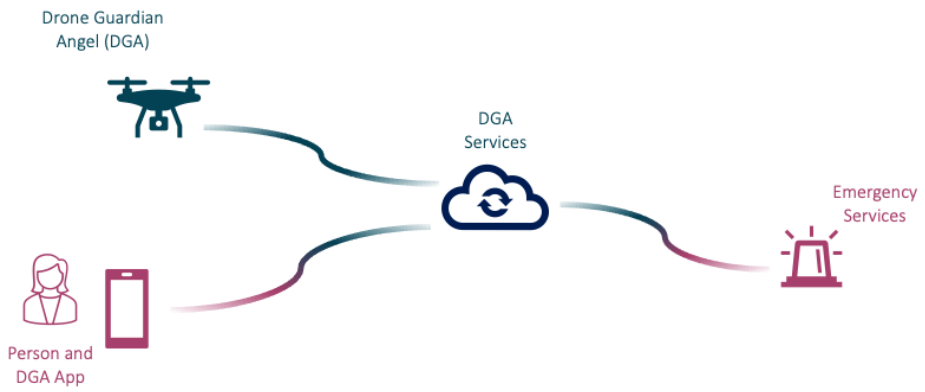

Figure 10 - DGA participant entities

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 the IoT service provider 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 (e.g. flying low over them, or in their direction), while it calls for rescue (DGA rescue first line service). If injuries are detected by the rescue service, a medical rescue team can also be called. While the rescue team(s) is/are on its way, some details can already be sent, collected by the camera and using the runtime geolocation, to give precise location and provide incident relevant information.

The deployment view of ARCADIAN IoT for DGA service, documented in D5.2 [5], is illustrated below.

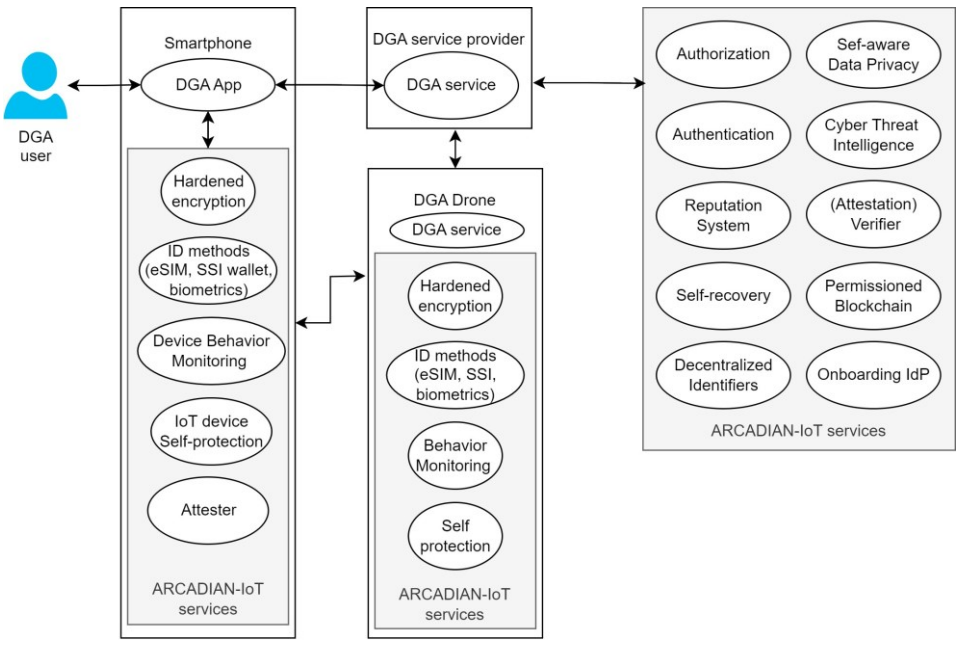

Figure 11 - High-level view of ARCADIAN-IoT involvement in Domain A

3.1.2 Use case A1 – Person Registration at DGA service

Overview

Before requesting a DGA service, the user must be previously registered at the DGA system.

The registration process for an end user to the ARCADIAN-IoT Drone Guard Angel service involves the user agreeing to the security and privacy mechanisms and providing personal data to be issued as a credential to their mobile SSI wallet and the creation of cryptographic keys for hardened encryption. For the latter, the user uses its smartphone to collect very basic personal data and to collect facial images from different requested positions (front, front-left, front-right, front-top and front-bottom).

The person registration process is concluded with the user presenting their previously issued credential from their mobile wallet to generate an associated ARCADIAN-IoT ID (aiotID) which is used to register the user with a second and a third authentication factors (the mobile network token and face biometric, respectively). Once successfully registered, a registration event is generated for which the user´s reputation is initialized.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Citizen / Person to monitor / 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 **mobile app** previously downloaded and installed in their smartphone. The registration steps are: 1. The user opens the DGA app and is presented with information from ARCADIAN-IoT framework referring security and privacy procedures included in the **service**. This means that, for example, the DGA service security **behaviour is continuously monitored.** 2. Willing to proceed, the person is informed that public cryptographic material for encryption of his personal data will be obtained and saved in his/her personal device **(Hardened Encryption).** Additionally, a key pair (one private and one public) will be generated in the RoT of the mobile device, assuming that the device has a SIM[3] with an ARCADIAN-IoT profile. The private key will be stored in the device RoT, ensuring tamper proof security for that information, while the public key will be sent to ARCADIAN-IoT key management system. 3. After, the user proceeds with the registration procedure, filling a form with the personal data needed for the DGA services, part of which is used for generating his/her **self-sovereign identity – SSI** (e.g., decentralized identifiers - non-centralized credentials that will allow to identify and authenticate him/her in the DGA services). The SSI ensures that no centralized

[3] Any SIM form factor, e.g., SIM, eSIM or iSIM

entity will own the full identify of the person, increasing thus its security.

4. The data provided by the person is encrypted with RoT information (the cryptographic material previously generated) and submitted to the DGAs services. The user is informed that they should make an encrypted backup of their Verifiable Credential in the users' SSI Wallet, allowing **credentials recovery**, in case of need. Is also informed that has the right to request the deletion of all his data. Is also informed that has the right to request the deletion of all his data. Is also informed that has the right to request the deletion of all his data.

5. The user is informed that the personal device **network credentials**, already at the device SIM, will also be used as a **second secure identification/authentication mechanism** in DGA services.

6. The DGA app now requests the SSI credential to be presented, continues with the registration and orders the creation of a person ID on the ARCADIAN-IoT Framework. The SSI Identity Provider (IdP) validates the signed HTTP Signature of the request and that it was signed by a Trusted Organization. Furthermore, the person's device reputation is initialized. To that end, the Reputation System, upon acknowledging the new registration, sends an Attestation Cue to the Remote Attestation's Verifier that in turn triggers the Attestation process. During this process, several device characteristics are appraised against reference values provided by the domain owner. The results are sent to the Reputation System.

7. To conclude the registration, and for the purpose of having **several simultaneous reliable identification mechanisms**, the DGA services ask the person to capture images to be used for **biometric identification** by authorized DGA drones. Images are encrypted with RoT material and sent to DGA services, where they are kept encrypted.

8. Finally, when the user identity is created, the device authenticates itself to the cryptographic key management service (**hardened encryption**) and obtains private decryption keys, that are saved to the personal device.

9. The person is informed in the app that the registration procedure is finished, and he/she can start using the service.

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.

Use case preconditions

1. DGA service organization is registered on ARCADIAN-IoT Trusted Organization Registry.

2. User has a smartphone with a SIM form factor (SIM, eSIM or iSIM) and the DGA app and SSI Wallet installed.

3. Remote Attestation (its Verifier component) has received the Reference Values from the DGA Service Provider, enabling future attestation of the smartphone once the DGA app is installed and configured.

4. (starts with the user acceptance of the terms provided within this use case) ARCADIAN-IoT behaviour monitoring component monitors 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/decryption 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 generated at the RoT of the user personal device. Information for decrypting user data is managed by the HE key management, which securely provides limited access keys to services and persons. The person authorizes the services to access his/her data. Personal data not in use is always kept encrypted. 2. User is requested to download SSI Mobile wallet and provides personal data needed for the SSI (Verifiable Credentials / Decentralized Identifiers) and is issued with a Person Verifiable Credential (VC) with personal identifiable information. The registration flow will now start in the user personal device with the user presenting the Person VC to be authenticated and result in ID Token sent to the DGA service, where it is sent in a request to authorise ARCADIAN-IoT services to create an ARCADIAN-IoT identity with a radio network token added by the network authorizer. Registered ARCADIAN-IoT Services create the aiotID and associate it with the SSI Person Identity and the Network Identity to be used for future authentications. An event is published on successful registration of the new ARCADIAN-IoT Identity to be consumed by ARCADIAN-IoT services such as Reputation System. 3. Biometric material is generated in the user mobile device, encrypted with RoT information and sent to the supporting ARCADIAN-IoT third-party services.

Implementation details

The implementation concerned the interaction of the Mobile App with the ARCADIAN-IoT platform for registering DGA service users.

A mobile App was created, including menus and functionalities for registration of the user, collecting login information, as well as minimal profile data (name, address, contacts) essential to the operation of all DGA features.

The collected data is inserted in a WebView where the interaction with the Decentralised Identifiers and Verifiable Credential components is made. As result of this, a token ID is received by the DGA backend, which will forward it to the DGA App.

The user is asked to confirm its registration in the ARCADIAN-IoT platform.

After the integration with the SSI component and the first step of registering personal credentials through is made, the App presents a flow of screens to collect 5 photos of the users' face in 5 different positions and, after user's confirmation, these photos are sent to the Biometrics components, where they are validated as useful images and stored to be used later as

authentication factor (described in use-case A2).

Additionally, the DGA App integrated a Remote Attestation module, via two different implementations:

- Ability to send Reference Values (e.g. App Signature) to the designated Verifier, via the framework's message bus (RabbitMQ);
- Integration of Attester package in the DGA App, periodically collecting info about the smartphone operation.

Finally, DGA App was integrated with Behaviour Monitoring or Hardened Encryption (via SIM) components, allowing all personal data to be encrypted and signed by the RoT using the HE component.

In each step of this flow, user-friendly and helpful feedback is given to the DGA App's user, not requiring any previous knowledge or training of the user regarding the actions to be done. Once the flow described above is completed and validated, the corresponding feedback is sent to the user.

3.1.3 Use case A2 – Person authentication at the DGA service

Overview

When a previously registered user opens the DGA Mobile App and intends to perform any action, the user needs to authenticate himself/herself via a multi-factor authentication approach leveraging **three robust identity mechanisms** to access ARCADIAN-IoT DGA services: biometric data, network identifier and SSI. After the authentication process is done, the user will receive feedback of the success or unsuccess of the action. This process will also apply in case the authentication token is expired.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane:** Security; Common.
Use Case Actors
Citizen / Person to guard.
Use Case Story
1. The user opens the DGA app and selects the login form. 2. The app informs that it will use the user SSI (**verifiable credentials)**, **network credentials** (in the smartphone SIM/eSIM) and **biometrics** for authentication. To proceed, the person needs to have an SSI wallet installed and take a photo. 3. If the user agrees, the **three identifiers** mentioned are used to login the user in the DGA services. In this process, the user is requested to present its Person Verifiable Credential in their SSI wallet. 4. If the three authentication factors are verified, the login process is successful and the DGA app is securely informed that the user is allowed to proceed. 5. If not, the process is not successful, and an error message is returned.

Relation with ARCADIAN-IoT Objectives
Objective 1: To create a decentralized framework for IoT systems - ARCADIAN-IoT framework. 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 preconditions
1. Use case A1. 2. ARCADIAN-IoT behaviour monitoring component monitors the behaviour of the device where the DGA is installed in order to trigger any security actions that are deemed necessary and update the trust knowledge. This may include system-level information (e.g., system calls), dynamic reputation and authorization changes for the device involved. 3. ARCADIAN-IoT Cyber Threat Intelligence (CTI) is running and able to receive threat alerts issued by the device behaviour monitoring component. 3. Remote Attestation's Attester sub-component is running on the device and performing periodic attestation.
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 DGA app requests the user to take a photo of his/her face and securely (e.g., using the **Hardened Encryption**) sends it attached to the authentication request. 2. Network identifiers are used according to the GSM standards. The novelty is that a protected network ID token is generated in the network core and attached to the authentication request. 3. Both the photo and the network ID token are verified to confirm if they are the expected identifiers for that person. 4. The SSI Person Verifiable Credential is presented from the user´s SSI Wallet in the smartphone and verified by the SSI Broker/Agent in the ARCADIAN-IoT platform with the obtained claims made available for the ID token. 5. A protected and signed ARCADIAN-IoT ID token is returned to the device for its authenticated operation.

Implementation details

This implementation concerned mainly in the interaction of the Mobile App with the ARCADIAN-IoT platform when dealing with the authentication of a DGA Guard user.

An authentication module was added to the DGA Guard mobile App, which includes:

- The developed mobile App enables the process of user authentication, starting by presenting a login form to the user.
- After this first step, a screen using the smartphone camera is presented to capture the

user's face in a front position.

- The data collected and the photo are sent to ARCADIAN-IoT Multi-Factor Authentication component, which will handle all the validation actions. The **Multi-Factor Authentication** component shares the person authentication results with other components. The **Reputation System** uses the positive (synonym of successful authentication) or negative results (failed authentication) to update reputation accordingly.

DGA App was integrated with Hardened Encryption (via SIM) components, allowing all personal data to be encrypted and signed by the RoT using the HE component. The app also integrated Device Behaviour monitor component, to monitor reputation changes and authentication events.

The results are used to craft a protected ARCADIAN-IoT ID token, which is returned to the mobile app for the user authenticated activity. The ARCADIAN-IoT ID is also shared with security- or trust-related components such as device behaviour monitoring (so that it can send threat alerts with respect to the device to other components of the framework) – and Remote Attestation – to support the attestation process. In each step of this flow, user-friendly and helpful feedback is given to the DGA App's user, avoiding any previous knowledge or specific training of the user regarding the actions to be done. Once the flow described above is completed and validated, the user is adequately informed.

The DGA Backend was also modified in order to intermediate and optimize some of the actions regarding data circulating between the Mobile App and the ARCADIAN-IoT platform.

3.1.4 Use case A3 – Person retrieving and editing personal data

Overview

After authenticating via a Mobile App (use case A2 flow), a user can check and/or edit the respective personal data in the App Profile area, Personal data that may be edited includes text-based fields as well as the face image used for facial verification / authentication purposes. Once the new data is collected, it is sent to the DGA backend. The result of the operation is then sent by DGA's backend to the personal device, being presented to the DGA user.

Use case description

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. In this case the story is: 1. When logged in the DGA app, the user requests to edit his/her personal data. In particular, the following fields can be edited name, address, phone number, SOS Contacts, and its identification photo images. 2. DGA services validate the requesting user, the requesting app and the personal device and assess the **reputation** of user, on which the request is performed. If the entities have the

necessary **authorization**, the encrypted data is retrieved to the personal device. 3. The user decrypts it with his private ABE key (**Hardened Encryption**). The data is shown to the user. 4. The user edits the intended fields and requests the sending of the data, encrypted again, to the DGA service. A **Hardened Encryption** process happens using ABE for encryption and RoT signatures. The updated data is kept encrypted and only accessible by the user and third parties registered in ARCADIAN-IoT, authorized by the user. 5. The result of the operation is shared with the ARCADIAN-IoT framework, in particular to the reputation system.
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.
Use case preconditions
1. Use cases A1 and A2. 2. ARCADIAN-IoT device behaviour monitoring component monitors the behaviour of the device where the DGA is installed to trigger any security actions that are deemed necessary and update the trust knowledge. This may include system-level information (e.g., system calls), dynamic reputation and authorization changes for the device involved. 3. Remote Attestation's Attester component is running on the device, supporting periodic attestations. To do so, the Remote Attestation's Verifier must have reference values and evidence appraisal policies, against which to analyse the evidence received from the device / smartphone to attest. These can be retrieved either from manufacturers or IoT service providers when the IoT service is registered in ARCADIAN-IoT. 4. ARCADIAN-IoT Cyber Threat Intelligence (CTI) is running and ready to receive threat alerts issued by the behaviour monitoring component. 5. The Reputation System is running and has initialized the reputation scores of the involved entities.
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).

Implementation details

A profile management module was added to the DGA mobile App, to allow authenticated users to access profile area for viewing or editing personal data. This includes editing written data, but also the user's face image associated to the profile, by going through the image capturing procedure used at registration stage (A1). The collected data is sent to the DGA backend, and the photo set is then sent to the Biometrics component to update its records.

DGA App leverages the integrations performed for A2, namely:

- Remote Attestation module, for periodically collecting info about the smartphone operational environment.
- Hardened Encryption (via SIM), allowing all personal data to be encrypted and signed by the RoT using the HE component.
- Device Behaviour monitor component, to monitor reputation changes and authentication events.

In each step of this flow a user-friendly and helpful feedback is given to the App's user, avoiding expert knowledge or training of the user regarding the actions to be done. Once the flow described above is completed and validated, the necessary feedback is provided to the user.

3.1.5 Use case A4 – Person Requesting a DGA Service

Overview

The core functionality of the ARCADIAN-IoT DGA service unfolds when users request a drone through the DGA mobile app, enabling them to seek personalized escort assistance by initiating a request for DGA services by sharing their GPS location and the location of the place they would like to arrive. This operational sequence seamlessly integrates secure technology and user-friendly interfaces, ensuring a smooth and efficient interaction for individuals who wish to avail themselves of DGA services.

Use case description

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. The key steps are: 1. Using the compliant DGA app, 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). 2. After verifying the user's identity, location, and the requesting app and device trustworthiness (via the **reputation** system), ARCADIAN-IoT DGA service selects a drone from the available ones – the drone itself is selected considering that **IoT device reputation** information. Drones' reputation can be formed considering factors like known vulnerabilities or dynamic knowledge built by ARCADIAN-IoT's **device behaviour monitoring** and **cyberthreat intelligence** components, as well as the attestation results generated by the Remote Attestation components.

3. The selected drone properties are retrieved and **attested**, assuring the device (and the DGA service) is compliant with the established reference values before granting it access to the user's personal data. 4. ARCADIAN-IoT DGA services share the necessary data (location), encrypted, with the drone. 5. The device, if trustworthy, is able to **decrypt the data**, 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 DGA services' customer if relevant, for a visual identification upon the devices' arrival to the service location. 6. The DGA service provides the basic information to start receiving video stream from the drone and identify the person that requested the service. The information is composed by URL video stream and the person identifier.
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 preconditions
1. Use cases A1 and A2. 2. ARCADIAN-IoT device 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. The Drone is registered in the system and its properties and reputation information are known and accessible. 4. RA's Attester component is running in the drone, supporting periodic attestations.
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.

Implementation details

Use case A4 implementation concerned mainly in the interaction of the Mobile App with the ARCADIAN-IoT platform when a user requested a DGA surveillance and vigilance service. The following implementation affected the DGA Mobile App, DGA backend and ARCADIAN-IoT platform:

- An App home screen was developed for the DGA mobile App, mainly composed of a map (based on Google Maps).
- In this map, input elements were implemented for allowing the user to confirm its current address and indicate its destination address (using Google API).
- Visual elements were implemented over the map to indicate the recommend path to follow

in that trip, with some information about duration of the walk, distance, drone's autonomy available for the service, etc.

- After checking all the info, the user can click on a button to confirm the trip request.
- Once the user requests a drone to a desired location for initiating the service, the necessary personal data is encrypted with RoT information and sent to the DGA backend.
- The drone selection, from the available ones, was implemented to consider the location and the reputation score (collected from the Reputation System), which itself builds from security-related information (i.e. device behaviour monitoring and CTI components).
- ARCADIAN-IoT DGA services backend share the necessary data (location), encrypted, with the drone.
- The user is then informed that a trustworthy drone has been selected and has been provided with the user's location and identification for performing the service.
- The DGA services backend provide the necessary information about an URL to provide video stream from the drone to the ARCADIAN-IoT platform, as well as the person identifier.

3.1.6 Use case A5 – DGA Service

Overview

After execution of use cases A2 and A4 and being granted with a service and having the necessary data, the selected (and trusted) drone needs to meet and identify the person that requested it, proceed with the vigilance service, and react in case of detected anomalies.

Use case description

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 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 steps of the story are: 1. The drone moves to the location of the requested service. 2. After arriving at the selected position, the drone informs ARCADIAN-IoT DGA services that it has arrived. 3. ARCADIAN-IoT DGA services inform the person that the drone has arrived, what is the device security and privacy **reputation**, and that he/she should get closer to it and allow **biometric identification**. 4. The person moves to the service location and allows the drone to identify her using the **biometric identification** described below. 6. The drone starts the **biometric identification**. For that, it can start streaming video to the DGA service securely. This data is only accessible by DGA services authorized by the user. 7. If trustworthy (according to **reputation**), the backend DGA services assign a URL identifying the streaming and the aiotID, to allow biometric component to access the video and perform

facial recognition of the user, with high accuracy Artificial Intelligence (AI) models. For privacy and security protection in this process, the AI component just receive images/content to perform the biometric identification and not the person identity (anonymization process separating the identity from the image recognition).

8. If the DGA facial recognition service identifies the user, a confirmation message will be sent to the backend DGA services, and from then to the drone and to the user. The user can then start walking.

9. If the person, personal device or app recognition fails 10 times in a row, it triggers DBM to alert for a (potential) brute force attack (DBM received these failure events directly from the authentication component). Then, the drone informs ARCADIAN-IoT DGA services and returns to the base. Such events, as well as the successful ones, feed the digital **reputation** of the user, personal device and/or drone through the **device behaviour monitoring** component.

10. When the process of identification is successful, the drone follows the user and, if anything abnormal (any event that can threat the physical integrity of the user) is detected by the drone's anomaly recognition system, data about the event is collected, and video streaming is started and **encrypted with RoT information** and sent to DGA services. In DGA services, the event data is decrypted for being analysed by an operator, who performs the follow-up measures needed. The user had to previously consent to the decryption of the personal data related with the vigilance service in the case of emergency (e.g., location and images captured by the drone) – **self-aware data privacy**.

11. The service ends when the user informs, using the app, DGA services, that it has arrived at the desired location and that the drone service is no longer needed. At the end of the service, 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 for his **privacy related self-awareness** 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 preconditions

1. Use case A4.

2. ARCADIAN-IoT device 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 required.

2. 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 at the user location, both the drone and the user personal device send their location and mutual authentication material securely, to the DGA services. 3. If successful, the drone captures the user biometric data (images or video), encrypts it and sends it to the Biometrics component through DGA services, where AI models are applied for person biometric identification. Biometric data is decrypted in Biometrics component and processed to ascertain if the identity of the user matches the authorized users. The verification result is communicated to the backend DGA services, based on which the service will or will not start. The other components of the user identity remain anonymous to the AI service, which just receives images/content to compare. If the result and the other identification processes are positive, the service starts, the drone and personal device behaviour is continuously monitored by the **Device Behaviour Monitor**, and service data is sent to DGA services encrypted. 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.

Implementation details

Use case A5 implementation concerned the interaction of the Mobile App with the ARCADIAN-IoT platform and the DGA Drone when a user requested a DGA surveillance and vigilance service. The following implementations affected the Mobile App level, DGA backend or ARCADIAN-IoT platform:

- The ability for the selected drone to take off from its base and fly towards the user's defined position (i.e. the location indicated when the service was requested).
- Once the drone arrives at the given position, it is able to inform ARCADIAN-IoT DGA services that it has arrived the location of the service.
- The user is also informed by the App to position itself where it can be easily viewed / located by the drone.
- A process of mutual authentication was implemented to allow the drone to collect biometric identification to send to ARCADIAN-IoT's Biometric component and request the identification of the targeted user.
- Upon the success of the mutual authentication:
  - the user is informed to start walking to the target destination.
  - the drone receives instructions to start the tracking user algorithm.
- A user tracking algorithm was implemented, to allow to follow the user according to its rhythm and potential slight deviations with respect to the initially planned path.

- The reidentification algorithm of the user was implemented, to allow to recover the target in case it disappears momentarily (e.g., being hidden beneath objects or structures such as trees which may appear during the path).
- The user status anomaly detection algorithm was implemented, to allow to detect any abnormal behaviour around the user that can cause any harm.
- When the trip ends with success, the user is provided in the smartphone's screen with a request to confirm the successful and safe arrival to the destination, upon which the drone can come back to the base.

When any anomaly was detected, a rescue team is called while the drone starts video streaming and flying around the anomaly happening scene. The return of the drone to the base will be ordered internally by the DGA services when the drone is not necessary anymore, and before its autonomy reaches the point of no return.

3.1.7 Use case A6 – Drone security and privacy incident

Overview

When under normal operation, the drone is subject to a security or privacy incident ultimately aimed at illegally stealing private information, compromising the DGA service or physically stealing the drone. Possible attacks which could fit the use case scope include cyber incidents such privilege escalation, Distributed Denial of Service, Network Mapper (NMAP) scans or Attempted Encryption of Large Number of Files (Ransomware).

Further details are provided in the use case story and the validation scenarios section.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Attacker(s), 3rd party entity (responsible for governing drone security)
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. The story related with the drone incident use case can be depicted as follows: 1. 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 **Device 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 both the device behaviour monitor's AI model on distributed information from the behaviours of devices in the network and the CTI's AI model on distributed information from local databases available to multiple CTI instances, while

ensuring **data privacy.**

2. For **protecting** the end-users' private information, the data is kept **always encrypted** and a **Remote Attestation** component is periodically attesting the drone making sure it fulfils the requirements to provide the service. Also, the **Reputation System** defines the device's trustworthiness according to several factors, including its behaviour, which is being monitored and analysed by the **Device Behaviour Monitor**. Only trustworthy devices receive vigilance services and related data, including cryptographic material for decrypting private data. As soon as a device is found to be not trusted, the RoT of the device will receive information over-the-air, from the network, to refuse to provide cryptographic material when requested by the compromised device. Moreover, its communication capacities are kept under control with a network-based **authorization** enforcement tool, which is always aware of all devices' **reputation**.

3. 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 – **SIM**/UICC (the **network credentials**), and a second one a **decentralized identifier**, not controlled or stored at any centralized entity.

4. 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 has no access to unauthorized 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).

Moreover, if the **Device Behaviour Monitor** detects the anomaly, possibly linked to a cyberattack, it sends an alert to the **CTI**, **Reputation System**, and **Device self-protection**. In turn, the **device self-protection** determines the appropriate security policies and either applies them itself or requests its application to the self-recovery component. Additionally, it informs the domain owner about the policy to be applied and informs the Reputation System about whether said policies were applied.

5. 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 on the ARCADIAN-IoT **blockchain** component.

6. When **the Cyber Threat Intelligence** component receives an alert, it will automatically update the information by adding the threat level and category associated with the alert. This updated information is then used to raise an alert for the CSIRT personnel through the GUI interface. Additionally, the IoC (indicators of compromise) identified in the alert is forwarded to other components within the ARCADIAN-IoT framework for further processing and response.

7. Reputation score updates published to the **Permissioned Blockchain** are available, on request, to external bodies such as Government Agencies or a client organization´s security auditor where security incidents on drones are subject to national law and/or client organization oversight.

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 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 preconditions
1. Drone is compliant with ARCADIAN-IoT[3]. 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 get damaged), not stolen and cooperative, the incident is mitigated, and its security and privacy are 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 about the device is gathered by the Remote Attestation component to attest the device's compliance with expected reference values. 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 to the person requesting it). 4. Data about certain aspects of the device behaviour is gathered and processed by the DBM continuously, to detect anomalous behaviour possibly linked to attacks. 5. Upon detection of an incident by the device behaviour monitor, information about the threat is sent to the device self-protection, CTI, reputation system. The device's reputation and its authorization are updated accordingly. Furthermore, the device self-protection determines the appropriate security measures and either applies them or forwards the policies to be applied by the self-recovery component. 6. In the case of a compromised device, that drone RoT is informed, over the air, of this and, from that moment until a successful recovery happens, the RoT will refuse to provide sensitive cryptographic material to the device. 7. In a recovery process, the app orders the recovery of the drone where its Decentralized Identifier keys are rotated on the blockchain component, and a new device fingerprint Verifiable Credential is issued to the drone, and network credentials are recovered from the network operator. 8. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating threat awareness. 9. Reputation score updates published to the Permissioned Blockchain are available, on request, to external bodies such as Government Agencies or a client organization´s security auditor where security incidents on drones are subject to national law and/or client organization oversight.

Implementation details

The backend supporting this domain has been adapted to integrate with security or privacy components of the ARCADIAN-IoT Framework (e.g., Device Behaviour Monitoring, Device Self-Protection, CTI). This allows for the components to monitor the drone and issue warnings or suggest protective measures.

3.1.8 Use case A7 – Personal device security or privacy incident

Overview

When under normal operation, the personal device is subject to a security or privacy incident resulting from a cyberattack (e.g. Replay Attack, Privilege escalation, Distributed Denial of Service, Attempted Encryption of Large Number of Files (Ransomware)).

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

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. The story related with these actions is: 1. 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 **device behaviour monitoring** component, and interpreted by the **cyber threat intelligence** tool. Also, for the same purpose, a **federated AI** paradigm will be in place to update the behaviour monitor's model on distributed data while ensuring the **data privacy** and supporting other components, e.g., of device and data protection and threat analysis. 2. 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 makes sure that the device characteristics are the ones required to run the app. Only trustworthy devices are authorized to request, from the RoT (**SIM**), cryptographic material. As soon as a device is found to be compromised, the RoT of the device will receive information over-the-air, from the network, to refuse to provide cryptographic material to the device. 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**.

3. 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 – **SIM**/UICC (the network credentials), and a second one an SSI (e.g., a **Verifiable Credential**), not controlled or stored at any centralized entity. The network credentials can be recovered with the network operator.

4. 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 doesn't have access to the RoT functionalities, hampering attempts of deceiving recipients with data from compromised devices. If the device is operational and cooperative, it takes actions for recovery from the incident according to the type (**self-recovery** component).

5. 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.

6. When the **Cyber Threat Intelligence** component receives an alert, it will automatically update the information by adding the threat level and category associated with the alert. This updated information is then used to raise an alert for the CSIRT personnel through the GUI interface. Additionally, the IoC identified in the alert is forwarded to other components within the ARCADIAN-IoT framework for further processing and response.

7. Reputation score updates published to the Permissioned Blockchain are available, on request, to external client organization´s security auditor where security incidents on the client´s end users and members are subject to client organization oversight.

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 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.
3. Wallet app must be previously issued with a Person Verifiable Credential (VC) and have been backed up to Credential Recovery.
4. The user is registered in the drone app.

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)
Person and IoT device.
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. Data about certain aspects of the behaviour of the device is gathered by the DBM continuously, to detect anomalous behaviour possibly linked to attacks 3. Upon detection of an incident by the device behaviour monitor, information about the threat is sent to the device self-protection, CTI, reputation system. The device's reputation and its authorization are updated accordingly. Furthermore, the device self-protection determines the appropriated security measures and wither applies them or forwards the policies to be applied by the self-recovery component, 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, its RoT is informed, over the air, of this and, from that moment until a successful recovery happens, the RoT will refuse to provide sensitive cryptographic material to the device. 5. In a recovery process, SSI credentials are recovered from Credential Recovery 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.

Implementation details

The backend supporting this domain has been adapted to integrate with security and privacy components of the ARCADIAN-IoT Framework (e.g., Device Behaviour Monitoring, Device Self-Protection CTI). This allows for the components to monitor the drone and issue warnings or suggest protective measures.

3.2 DOMAIN B – Grid Infrastructure Monitoring

3.2.1 Application domain context

Grid domain is generically defined by critical infrastructures covering electrical energy, utilities and correlated environment. Monitoring of infrastructure elements (based on their role into architecture, typology or displacement into field) is either done by SCADA systems, or by local / isolated technologies or not at all. Industrial IoT technologies, operating with microcontroller powered devices and cloud platforms are a good mitigation tool to monitor the unmonitored elements and retrofit the isolated / not modernized monitored elements.

Due to sensitivity of data, it is highly demanded a cybersecurity technology matching both a solid state of data integrity, lack of exposure and limited computing capacity of Microcontroller Unit powered devices. So, it was designed a security system, hardware encryption base, which carry end-to-end data between sensors and managing IoT platform.

The deployment view of ARCADIAN-IoT for GMS, documented in D5.2 [5], is illustrated below.

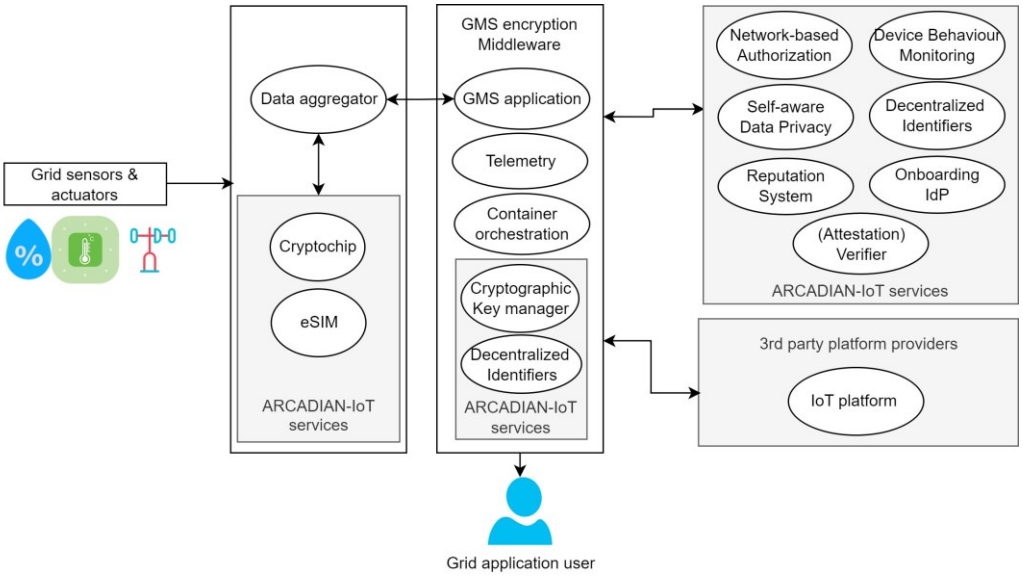

Figure 12 - High-level view of ARCADIAN-IoT involvement in Domain B

3.2.2 Use case B1 – New Device Registration

Overview

This use case considers the registration of a new IoT device into the ARCADIAN-IoT framework, and the bootstrapping of the framework's services required for monitoring its security. It involves the acquisition of the required information for the registration – such as cryptographic data; the actual registration in the framework; and the consequent initialization of ARCADIAN-IoT's services and the device's reputation.

Use case description

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

Use Case Actors
Grid infrastructure manager / authorised operators
Use Case Story
This use case depicts the scenario of the service supplier configuring and registering a new IoT monitoring device that is supported by ARCADIAN-IoT to gather and propagate information from sensors and actuators of a grid infrastructure, with security and privacy, to a monitoring tool and an IoT platform managing sensors data. The story steps are: 1. In the grid monitoring device assembling, besides the firmware adapted to each grid infrastructure needs, each device is setup with a **crypto chip** and an UICC for receiving **SIM** 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). In this case, the SIM component will be used to provide cellular connectivity and to allow a network-based **authorization** enforcement of the device according to trust policies (from the **reputation system**). 2. After the device robust identifiers (keys) are generated and provisioned to the device, together with DIDs and Device ID, user and password, the device is ready for performing the hardened encryption (having the cryptographic material to encrypt/decrypt the sensitive data and its firmware programmed running such). 3. The device is registered in the ARCADIAN-IoT framework by a signed request from the Grid Management Service (GMS) middleware which is verified by its DIDs public key and the DID being previously registered in the Trusted Organization Registry. These services bootstrap the device processes of **Authentication, Reputation System**, and **Device Behaviour Monitoring** in ARCADIAN-IoT framework. 4. Upon this registration, the **Reputation System** sends an attestation cue to the (**Remote Attestation**) Verifier to attest the device, comparing its claims to the reference values provided by the domain owner beforehand. 5. Through a reliable web interface, the GMS middleware informs the infrastructure manager[2] 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 (such as Orchestra Cities of Martel, standalone container of **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 its data security and privacy. 6. If the infrastructure owner accepts the connection of the device to the IoT platform managing the sensors data and to ARCADIAN-IoT framework, the GMS setup is ready to securely connect grid infrastructure sensors and actuators to one (directly) or more (through the main one, by API) IoT platforms managing the sensors data (through the GMS IoT device and middleware).
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.
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 system with identification and authentication mechanisms compatible with ARCADIAN-IoT. 3. Reference values for each registered device (device claim) were sent to the Remote Attestation's Verifier to support the appraisal of evidence during the attestation process. 4. Upon the manager acceptance, the ARCADIAN-IoT Device Behaviour Monitoring component is continuously monitoring the interactions of this domain's registered devices, remotely, through the Middleware. 5. Each IoT Device has a DID:WEB hosted by the middleware platform. 6. The GMS System is registered in the ARCADIAN-IoT framework´s Trusted Organization Registry with its associated DID:WEB.
Use case postconditions
1. GMS IoT device is supported by 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 respective telemetry / grid infrastructure monitoring / IoT platform and start communicating data. 3. Remote Attestation is performed successfully – i.e., the evidence was evaluated, and an attestation result was generated. 4. Device Behaviour Monitoring component is monitoring the newly registered device's behaviour, through the Middleware, to trigger any necessary security actions and updating the related trust knowledge (which may include reputation and authorization changes). 5. The infrastructure owner is aware of where his data will start being sent, authorizing specific third-party monitoring tools / IoT platforms. 6. The infrastructure owner is aware he could use other security systems part of ARCADIAN-IoT security framework, for its infrastructure, by adoption of system as it is, SaaS or on prem, or by technology transfer between partner and its internal entities responsible for this, using other applications.
Entities/Scope (Person/IoT/Apps Services)
All
Data used and data flow
1. The network-based identifier is provisioned to the device using the SIM GSMA-SAS standards and stored at the UICC, which is a secure element. 2. The cryptographic material for hardened encryption, generated at the crypto chip, and defined in crypto chip repository and Middleware HES data base. 3. Upon authorization from the infrastructure manager, the device authenticates in the

Middleware (using keys dedicated for this stage). 4. The device's behaviour starts being monitored by the device behaviour monitoring component. 5. The device's reputation is initialized by an initial attestation process requested by the Reputation System to the Remote Attestation and by the fact that Device ID was previously defined into Reputation System data base, for registration purposes, and linked to device reputation policy from Reputation System.

Implementation details

Usage of multiple IoT / monitoring platforms is possible across devices lifecycle, conditioned by a main / default one connected with Middleware, which will terminate the sensors data, but could forward these data sets through customized APIs to multiple destinations. In this way, the whole security chain is maintained end-to-end, because the default IoT platform will use TLS for API communication with the others. Process of mapping Device IDs and IDs of sensors and actuators connected to it, stays with 3PP IoT platforms managers / authorised operators.

A Verifier with the Middleware's API was implemented to support Remote Attestation.

Integration with Device Behaviour Monitoring and Self-aware Data Privacy involves previous sharing of Device IDs in scope of monitoring on RabbitMQ established interfaces with these systems.

A policy document and Device IDs in scope of monitoring must be provided to Reputation System operator, for provisioning within this.

Process of registration was tested and optimized to run smoothly with a trained operator.

Process of registration is called at new device onboarding, and whenever a device was compromised and requires a new provisioning of security elements, on the previous used hardware.

3.2.3 Use case B2 – GMS IoT device data gathering and transmission process

Overview

In this use case, IoT device transmits sensors data, named also "data traffic", in a secured way to an authorized IoT platform. The Middleware (a cloud software component) must be capable of relaying the received encrypted traffic from IoT device to any IoT platform authorized to use sensors' data. Relaying of traffic takes place after decrypting data with a correspondent key generated by the crypto chip (previously provisioned) and encrypting data by TLS before transmitting forward to IoT platform.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Grid infrastructure manager / authorised operators.
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. The main steps are:

1. After getting and aggregating the data from the grid infrastructure sensors the GMS IoT device performs the **hardened encryption** of the payload with Root of Trust – crypto chip – information, which is the encryption key provisioned for device traffic. 2. ARCADIAN-IoT **Device Behaviour Monitoring**, oversees and interprets the IoT device behaviour through GMS middleware, which adjusts the device security and privacy **reputation** and its **authorization** to access or be accessed by online services when needed. 3. GMS middleware **decrypt** the device traffic with corresponding provisioned key, and relay it **encrypted** by TLS to the IoT platform used for sensors data management. 3. According to the GMS monitoring rules and the infrastructure manager authorization, GMS middleware forwards the data to the IoT platform handling sensors data, and optionally to other compliancy monitoring tools (Orchestra Cities of Martel, standalone container of **Self-aware data privacy**) by API. These third-party tools need to comply with ARCADIAN-IoT to be able to decrypt the GMS data[4]. TLS encryption will be used for API communication between GMS middleware and any of IoT platform, compliancy monitoring tools. 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 Device ID, Device unique credentials (user, pass) and crypto chip allocated key**. Once this authentication is done,** the device starts to run its local sensors reading cycle (by edge firmware agent) and encrypt the traffic with another crypto chip allocated key for this stage. 5. 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.
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 components oversee the interactions of the IoT devices 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, IoT platform managing sensors data and any other authorized monitoring tool. 2. Every single data transmission is encrypted, following the process automatically. There are no data sets in clear.
Entities/Scope (Person/IoT/Apps Services)
IoT / Apps Services.
Data used and data flow
1. The device identifiers and authentication material, cryptographic material for hardened encryption and TLS 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. 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., Device Behaviour Monitoring) to infer potential threats and act if needed.

Implementation details

A focus was kept for using multiple type and format of sensors data; using various defined periodicity of transmission (1min, 5min, 15min - regular industrial telemetry periods), per each sensor (e.g., of tested sensors interfaces: Modbus, M-Bus, Pulse, 4-20mA, 0.5V DC, 0-10V DC), to stress the device awakens capabilities; using multiple telecommunication technologies (GSM, LTE, LTE-M, ETH), to validate the field challenges; 0(zero) tolerance to failed encryption or not performed / skipped encryption by device firmware; verifications for each data set to reach the IoT platform and other monitoring applications. Samples of data sets used are production, consumption, quality or behaviour of energy, environment, polluters concentration, behaviour, debits of industrial fluids.

3.2.4 Use case B3 – Service request from third-party IoT monitoring platform

Overview

In this use case, an IoT platform, handling GMS IoT devices data, transmits a command for a chosen IoT device, based on Grid manager / authorised operator decision.

Scope of the command is to actuate / switch a grid field control element through GMS IoT device, by using an encrypted end-to-end path, by the Hardened Encryption System.

There are 2 security segments involved, one from IoT platform to Middleware, and one from Middleware to targeted GMS IoT device. Bounding / relaying of the command information, maintained into a security format, stays with Middleware capability.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Security; Common.
Use Case Actors
Grid infrastructure manager / authorised operator
Use Case Story
Management of grid infrastructures involves sending commands to the field elements, by IoT devices where their controllers are triggered from. An example can be the request to change the status of an electrical contactor of a substation feeder, or of a pumping system. In this case, a use case story with ARCADIAN-IoT participation is: A grid infrastructure manager / authorised user authenticates in the IoT platform with a compliant multi-factor authentication and credentials. 2. When successfully logged in, the user selects a GMS IoT device from the grid infrastructure he has access to, and requests to send a predefined command to that device, for a certain port belonging to it. On that port, into field, it is physically connected the field control element (e.g., contactor). 3. Once command is sent, the IoT platform will send via TLS to the Middleware the request. The Middleware (connected via API with IoT platform) will decrypt the request. It will take the command string and encrypt it again, using Hardened Encryption System, by choosing the Device ID where command must be sent, and by choosing the encryption key, previously defined and dedicated for this Device and to this type of operation. 4. Middleware will send the encrypted command to that specific Device ID. GMS IoT Device, once receives it, extracts locally from its encryption repository, by firmware encryption agent,

the key correspondent with the operation type. This key, if it is not similar with that one used by Middleware, will not be capable to unencrypt the command received. With the proper key, part of RoT (crypto chip), command is read in clear by GMS IoT Device firmware, and local control firmware block will identify the port and the type of change and apply it. After a delay (set up previously, into firmware config), the firmware will check the status of the engaged port and will transmit back to IoT platform – as a B2 use case – the feedback of command (changed accordingly / not changed). This is for authorized user evidence / control, in relation with managed grid infrastructure. Lack of feedback is interpreted as a failed command. To preserve the security of grid infrastructure, it is no retry implemented. A new command request must be performed, and process will run again completely. 5. Even if it was successful or unsuccessfully decrypted by Device, this one will always inform Middleware about. 6. Middleware updates RabbitMQ, mainly to provide the Device Behaviour Monitoring System and Reputation System systems events for consumption.
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.
Use case preconditions
1. Use case B1. 2. Grid infrastructure manager / authorised operator registered in the Middleware with an identification compliant with an ARCADIAN-IoT person identification. 3. IoT platform integrated with Middleware via API (compliant with ARCADIAN-IoT). 4. IoT platform provisioned with IoT devices relevant information (ID, sensors, commands, triggering values for alerting and command, etc.). 5. ARCADIAN-IoT Device Behaviour Monitoring, reputation system and CTI components oversee the devices and third-party service 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 and informs the Middleware about success too. 2. If the operation is not successful, the device continues with the previous routines, but informs the Middleware about failed command execution due to lack of key (RoT crypto chip) matching. 3. In any situation, IoT platform which sent the command will receive feedback about. This is for the reason of operations within Domain B – grid best practices.
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 / authorised operator (person) credentials, IoT platform HTTPS certificate (for establishing TLS session with Middleware), GMS IoT device identifiers, its current configuration and its new configuration, and cryptographic material (key) for encrypting/decrypting the command. 2. Using an ARCADIAN-IoT compliant IoT platform, a user requests a command to be executed into a specific device. Being authenticated and having the necessary authorization, the information is sent by IoT platform through the Hardened Encryption System, to the targeted end point, the GMS IoT device. 3. At the device, the command is decrypted with RoT information and, if successful, applied. 4. If the device is unable to decrypt the data, informs GMS middleware and discards it.

Implementation details

GMS IoT device got deployed a feedback mechanism, to notify the IoT platform if the command was executed. Feedback notification is a standard B2 use case, but always triggered internally into GMS IoT Device firmware by a B3 use case.

Implementation was performed using real field elements and following the dispatching logic of Regional / National Dispatching bodies of grid DSO (distribution system operator) / TSO (transmission system operator).

It was used BOX2M Industrial Telemetry Platform as IoT live production platform, to play the IoT platform role. Any other MQTT & TLS equipped IoT platform, vendor independent, could play similar role.

3.2.5 Use case B4 – GMS IoT device security or privacy incident

Overview

The work done to achieve the goals of use case B4 was related to the features allowing the Hardened Encryption System to be aware and act on security incidents occurred on IoT device, with support of the other integrated security systems.

These could be due to, for example, failed encryption at the GMS IoT device level due to keys mismatching. B4 is applicable for both ways of communication involving GMS IoT devices (authentication, sending sensors data to IoT platform, getting commands from IoT platform).

Use case description

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. This can include situations when device, due to an attack of middleware or of its entity, fails the authentication, the traffic transmission or the commands requests from an IoT platform. Attacks could change the correspondent encryption keys or disable the correspondent service. Middleware is permanently connected to ARCADIAN-IoT RabbitMQ and provides updates to Device Behaviour Monitoring every time when devices are running an operation involving data transmission or receiving to/from IoT platform managing the sensors and actuators data. 1. During authentication, due to a firmware potential intrusion or even a provisioning mistake done into device firmware, during registration (initial onboarding), if the keys provisioned for authentication stages are not matching the keys defined at Middleware Hardened Encryption data base, device will be rejected from getting authenticated / authorized. Middleware will notify this error message and update the Device Behaviour Monitoring. The component will consume the message, having forward liberty for further actions. In parallel, Middleware notifies the Reputation system accordingly, and this one applying the defined policy, will downgrade the

reputation of the correspondent Device ID.

2. Still part of authentication, with wrong DIDs, it will be generated a similar action, but in this case, regarding Reputation, Decentralized Authentication security system may inform the Reputation system, on top of what Middleware does anyway.

3. During traffic transmission, because sensors data are encrypted with a different unique assigned key per Device ID (traffic key), even if Device was properly authenticated, but the traffic key is wrong, then Middleware interprets this as an error, rejects the traffic, updates the Device Behaviour Monitoring queue regarding the incident, and keeps updating the Reputation system.

Another significant example, as traffic transmission, are the devices' claims, which are sent to the Remote Attestation's Verifier as encrypted traffic (to attest the devices). Being a traffic type message, if it is not transported correctly via Middleware, and via API of IoT platform to Remote Attestation system (which involves a successful encryption end-to-end process), this one will not be able to verify the claims, so device reputation will be degraded, and forward actions may be deployed by ARCADIAN-IoT framework (up to requesting to Middleware to refuse Device ID reconnections until further updates). This situation, involving a failed encryption due to wrong keys matching, will trigger a similar Device Behaviour Monitoring incident, as for any other traffic transmission.

4. In case of a command sent by IoT platform, if the decryption fails on device level (due to the same reasons mentioned above, as unique keys provisioned on device for this type of operation not matching Middleware correspondent keys, by an attack or a provisioning mistake), command will not be read in clear by device firmware module responsible with actuation / actions on local ports, so will not be executed. Middleware will notify the lack of feedback from device, after command was sent, on top of notifying the failed decryption information, and run its routine accordingly, with Device Behaviour Monitoring and Reputation System.

Even when these steps are running successfully, **without generating incidents**, the Device, through Middleware, updates the Device Behaviour Monitoring queue.

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 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, decentralized authentication, remote attestation, behaviour monitoring) are operational.

3. All use case actions will take place only if the GMS IoT device is previously authenticated

and connected through a data network (mobile, fixed).
Use case postconditions
1. If the device is operational (e.g., did not get damaged) and not stolen, the incident is mitigated, by correct reprovision of impacted keys and its security is restored. A best practice could be to have the whole Device set of keys changed, both in Device encryption agent repository and in Middleware data base (preventing a situation where an attacker copied the keys associated to the incident). 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 / Apps
Data used and data flow
1. Device and IoT platform regular data sent / received, for lifecycle operations, generating information from point #2 (below listed). 2. Periodical information to attest the device identity and integrity, and traffic performing / command received, as messages consumed by Device Behaviour Monitoring system. 3. IoT device belonging behaviour data (consumed by CTI and DBM to understand potential threats or incidents). 4. The CTI tool shares threat information in the form of trained models with CSIRT and CERT networks for propagating the threat awareness.

Implementation details

To strengthen and simplify the security process, the Device Behaviour Monitoring system was integrated with the Hardened Encryption system provider (GMS Middleware) via RabbitMQ, aiming to enrich / optimize the IoT devices profiling of incidents. This was integration was crucial for the detection of IoT device incidents and it directly supports the execution of B1, B2 and B3 which the respect to detection of device incidents. To properly attest the devices, the Hardened Encryption System also builds from the integration with the Remote Attestation (performed for previous use cases).

If the Middleware is out of service, processes cannot run. As a work around, and if it is legally / formally authorised by Grid customer, previous to the fulfilment of Device firmware and correlated Middleware configuration, a hard copy (nonelectronically) of encryption keys for its fleet could be provided by GMS IoT vendor. In case of keys replacement for Devices which experienced too many incidents, this list must be updated too.

If the Middleware does not run, commands cannot be dispatched to any of IoT devices, and no IoT device can communicate with the IoT platform, so the Grid risk is reduced until recovery. This makes Hardened Encryption System a strong “2nd path” monitoring and control, against legacy SCADA systems.

3.2.6 Use case B5 – GMS middleware security or privacy incident

Overview

The work done to achieve the goals of use case B5 was related to the features allowing the Hardened Encryption System to be aware and act on security incidents that have occurred on Middleware software platform. Incidents could be due to failed encryption run by the Middleware (due to lack of correlation with information provisioned into the IoT device or the IoT platform). B5 is applicable for both ways of communication involving the Middleware (sending sensors' data, getting commands), and to both encryption technologies used by Middleware (TLS certificates and hardware encryption keys), due to failed authentication of Middleware to API / RabbitMQ interfaces provided by other security systems or due to failed authentication of authorized operators at Middleware login page.

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

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., API, RabbitMQ – interface logins with other security systems). 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. Middleware is permanently connected to ARCADION-IoT RabbitMQ system and updates the queue of the reputation system if there is an incident where it is involved. 1. During traffic transmission, because sensors' data must be received by IoT platform handling such data, the Middleware uses the dedicated API interface with that IoT platform. Out of service status could be generated by networking reasons (cloud infrastructure unavailability or congestions, interfaces, firewalls claim), TLS failed encryption process, API login process, IoT platform wrong provisioning (by changes applied across lifecycle), IoT platform itself availability. 2. During command requests process, considering IoT platform is generating such commands, the Middleware will use the same dedicated API interface with that IoT platform. 3. In parallel, Middleware provisioning and maintenance require authorised and trained users (from Grid or from system integrator deploying the technology for Grid, both with close support of vendor providing the Hardened Encryption System). Users have credentials and a 2-factor authentication service in place for getting access to Middleware, on top of rights and permissions previously assigned within credentials definition process.

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 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., HES, reputation system) are operational. 3. IoT platform has API up & running with Middleware. 4. Authorised users are provisioned and active on Middleware.
Use case postconditions
1. Related to API, once incident is resolved, if the root cause showed it was not an infrastructure reason, a best practice could be recreation of API, with other credentials, both in IoT platform and in Middleware side. 2. Related to users, repetitive failed login trails should be investigated. If a user is untrusted, his access should be erased. Optionally, if this one had extensive rights (visibility on keys), keys reprovision process should take place (which corresponds to Use case B1).
Entities/Scope (Person/IoT/Apps Services)
All
Data used and data flow
1. Device and IoT platform regular data sent / received, for lifecycle operations, generating information from point #2 (listed next). 2. Periodical information to attest the Middleware identity and integrity, and traffic performing / command received. 3. Users credentials and TLS certificates for API. 4. Periodical information sent to Reputation System, by Rabbit MQ messages, about API status.

Implementation details

Middleware incident detection within ARCADIAN-IoT operates based on reputation score changes with respect to the Middleware. The Reputation System processes Middleware-related events and computes reputation scores. Under this scenario, a system administrator can monitor the status of Middleware. The technical implementation for this domain required the collection of events and respective forwarding to ARCADIAN-IoT RabbitMQ to feed the reputation system.

In addition, partners have verified that is technically possible to provide access to the System Calls of the Middleware execution container to the Device Behaviour Monitoring, which in turn could detect anomalous events in the system. Nevertheless, the required security policy settings for the container deployment (i.e., deployment mode of the container in Kubernetes for the system calls to be available) are not currently adequate for the Grid Domain.

As part of the use case development, in parallel to integration with ARCADIAN-IoT components, it was possible to collect and generate Middleware related events (e.g., operation status, operation, and others) and enable the forwarding to a message bus such as ARCADIAN-IoT RabbitMQ. This leads to additional monitoring capabilities that are that are not part of ARCADIAN-IoT project but can be added on beyond the project completion.

3.2.7 Use case B6 – External data audit to grid infrastructure

Overview

The work done to achieve the goals of use case B6 was related to the features allowing an authorised operator (belonging to a state authority or an empowered entity) to recover encrypted data from a recovered device. IoT device was supposed to has disappeared for a while from monitoring or get exposed under uncertain conditions related to its physical security / site access. This use case does not require any security system integration, but it is a European Union Agency for Cybersecurity (ENISA) recommendation for any hardware security vendor which stores sensors metering data.

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust. **Horizontal plane**: Common.
Use Case Actors
Authority agent, Grid infrastructure manager / authorised operator, GMS IoT vendor.
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 a specific incident (physical security sabotage, reported not allowed physical access at device or its containing site, lack of access on device from monitoring platform correlated with other factors). An authorized body (Authority), 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. The story is the following: 1. Upon request from an authorized body, the GMS technology vendor provides an auditing tool

(hardware and software) that allows to retrieve the data stored in a GMS IoT device, and specialised assistance together with offline notification of involved bodies. For data protection purposes, just specifically authorized and identified devices and services can retrieve such data. 2. The agent from the authorized body (Authority) will have access on suspected GMS IoT device. He needs to connect the hardware auditing tool to device designated port, and to identify and authenticate himself/herself in the provided software tool by IoT vendor (e.g., with **eIDAs** or **VC**), in the presence of the grid infrastructure manager. Credentials for device login will be provided by vendor (without being exposed / shared in clear, just typed into console opened by Authority). 3. The grid infrastructure manager / authorised operator will login to Middleware, identify the unique encryption key assigned for Use Case B6 of the device in scope of investigation, and provide this key to the Authority agent. 4. With the key provided, fulfilled into IoT vendor software tool, the Authority can export the buffered data from device EPROM to an Authority external offline destination (hard disk, memory stick), as probes for further investigation. These data represent the not transmitted sensor data during disconnection of device from IoT platform (during supposed sabotaged), may representing a part of the scope of Authority investigation. 5. Once this operation is finished, The IoT device vendor may notify (by a secured mail) the Reputation system owner (manager / authorised operator), to remove forever the suspected Device ID from its data base. Reputation system owner will have to confirm with Device ID vendor and with Authority from the authorized body, before executing the data erase. Even if "no data" were stored on EPROM, use case still stands, because a sabotaged device must be eliminated and recreated, to preserve the Hardened Encryption System root of trust, across operations lifecycle. 6. The GMS IoT vendor will remove forever (not using again in the future), from Middleware, the Device ID, correlated unique credentials and encryption keys used for all stages. 7. The GMS IoT vendor will remove forever, the suspected GMS IoT Device firmware. A new firmware can be provisioned on the hardware platform, according B1 use case scenario. This task is done to make sure, during supposed sabotaged, the firmware structure and code were not affected too, on top of stored sensors data.
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 preconditions
1. Use case B1. 2. Grid infrastructure manager / authorised operator have identification credentials compliant with ARCADIAN-IoT persons identification. 3. Unique and dedicated encryption keys for this use case are provisioned into Middleware and GMS IoT Device firmware. 4. Audited GMS IoT device had an incident that demands auditing. 5. ARCADIAN-IoT framework reputation system component is operational.
Use case postconditions
1. Auditing process finished. 2. Data from the auditing process deleted from auditing tool. 3. GMS IoT device firmware and correlated Middleware config must be erased and never used again, before GMS IoT device 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 grid infrastructure is sent to the ARCADIAN-IoT framework authentication component. If the persons, the device and the software it runs are found trustworthy, the operator can authenticate in GMS with the software auditing tool.
2. The Authority agent 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 / authorised operator and by the IoT vendor.
3. If authorization is provided, the data that is stored encrypted in the device is retrieved by the software 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 software auditing tool, with the authorized operator authenticated, decrypts the data, and makes it visible to him/her. Data is read-only.
6. At the end of the process, all the data and cryptographic material is automatically deleted from the auditing tool.

Implementation details

To strengthen and simplifying of security process, Authority agent relies on Grid and GMS IoT vendor support, to perform the legal requested operations, without owning dedicated credentials into Hardened Encryption System.

If the Middleware is out of service, the process cannot run. As a work around, and if it is legally / formally authorised by Grid customer - before the configuration of Device firmware and correlated Middleware configuration - a hard copy (non-digital) of the encryption keys for its fleet could be provided by GMS IoT vendor.

3.3 DOMAIN C – Medical IoT

3.3.1 Application domain context

The application domain of Medical IoT focuses on monitoring patients at their homes, emphasizing the importance of sustainability in health systems and the comfort of monitored individuals. IoT solutions in the medical field, such as telemedicine sensors, facilitate remote patient monitoring, allowing for personalized and efficient healthcare delivery. However, the utilization of IoT for medical purposes, needs stringent measures to address data privacy and security concerns effectively.

In the context of ARCADIAN-IoT Medical IoT (MIoT), a typical scenario where patients receive personalized treatments, telemonitoring system could be used to reduce the number of consulting sessions, benefiting both medical staff and patients. This solution provides an evolutionary record of patients' status automatically.

The Medical IoT domain within ARCADIAN-IoT emphasizes a patient-centric approach to healthcare delivery, aiming to enhance the quality of care, optimize treatment outcomes, and ensure the privacy and security of patient data throughout the monitoring and treatment.

The deployment view of ARCADIAN-IoT for Medical IoT service, documented in D5.2 [5], is illustrated below.

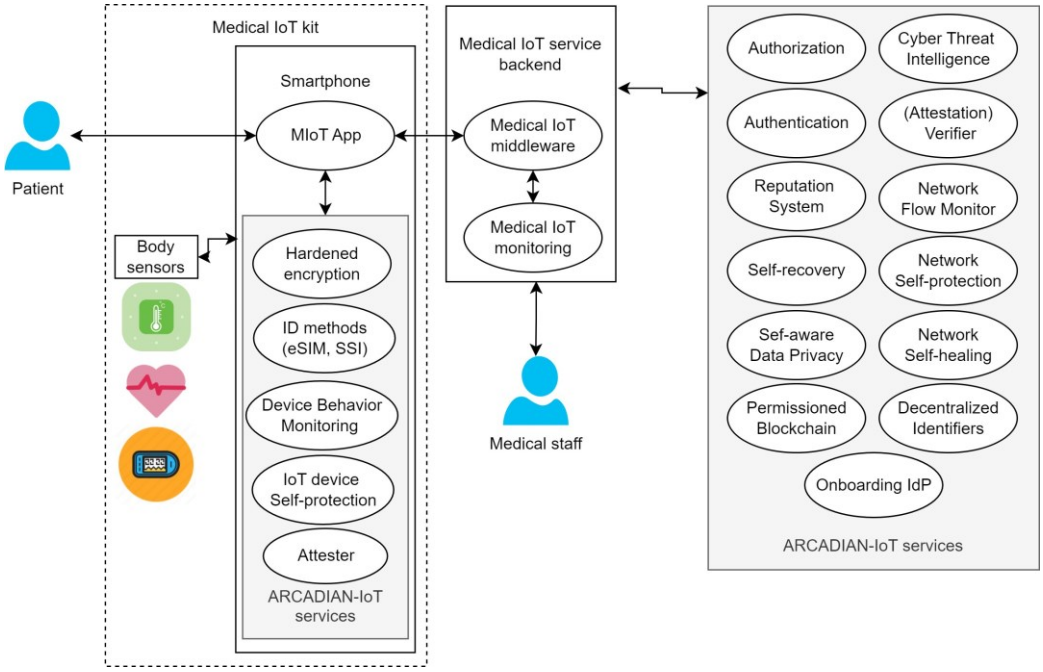

Figure 13 - High-level view of ARCADIAN-IoT involvement in Domain C

3.3.2 Use case C1 – MIoT kit delivery – Patient registration and authentication

Overview

This use case depicts the scenario of the enrolment of a new patient to be monitored at home with the 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 synched with the smartphone).

An authorized medical professional (doctor, nurse or other) requests the patient to register

themself using the MIoT app, in a smartphone that is going to be assigned to the patient. At this stage the device is completely free of any personal data of previous patients.

Use case description

ARCADIAN-IoT Layers
Vertical plane: Identity; Trust; Recovery. **Horizontal plane**: Privacy; Security; Common.
Use Case Actors
Patient and Medical professional.
Use Case Story
When the person opens the MIoT app is presented with information from ARCADIAN-IoT framework referring that the **service terms** in what regards data security and privacy procedures. This means that, for example, the security behaviour of that device, of the MIoT app and of all the MIoT services are continuously monitored (**device behaviour monitoring** and **network flow monitoring**) and interpreted **(CTI** and **self-protection components)** and have initialized the trustworthiness **reputation** score. The security reputation of the MIoT entities involved is presented to the patient at this moment. With the patient authorization, cryptographic material for ensuring trust in the communicated data 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. The data provided by the person is encrypted with RoT information and submitted to the MIoT services. The app continues the registration of the patient and requests the patient present their Person Verifiable Credential from their SSI Wallet. The user presents the requested credential from their SSI Wallet and the app performs a signed registration request to the ARCADIAN-IoT framework for the patient including the network token from the mobile core network and an identity token created from the Person VC. The registration request is validated that it is performed by a trusted organization, with the DID that signed the request verified that it is registered in the Trusted Organization Registry, on the **Permissioned Blockchain**. If the request passes validation, an aiotID is generated in the framework and an event is raised so that components in the framework (such as Reputation) are aware of a new registered Person. The patient is informed that his/her new network credentials, associated with the **SIM/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. Upon completion of the registration of the patient in the smartphone, ARCADIAN-IoT **Reputation System** sends a cue to the Remote Attestation which triggers a first attestation process; consequently, the Attestation Result is processed for determining an initial estimation of the device's reputation. 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 (see use case C4), can see that the patient is correctly enrolled in the system and the device 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 get access their 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 skills, this process 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. At this stage, the patient is registered, and the equipment is configured to start being used in his/her home.

At home, for authentication, the MIoT app requests to retrieve the user´s Person **Verifiable Credential** from the SSI Wallet. For secure access to the wallet itself, a biometric factor may apply (e.g., fingerprint).

If permission is given, **identification and authentication** data is retrieved and used to login the user in the MIoT services based on SSI and mobile network token authentication factors. The app itself also presents its identification to the services (namely to interact with the **SIM RoT** when needed).

If the user, the smartphone and the app are authorized to access MIoT services, including being trustworthy, according to the **reputation** model, 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.

Use case preconditions

1. MIoT services and app are integrated with ARCADIAN-IoT components.

2. Medical staff is registered in MIoT monitoring services with ARCADIAN-IoT identity management services.

3. 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).

4. ARCADIAN-IoT device behaviour monitoring and CTI components start overseeing the device behaviour to trigger any necessary security actions and updating the related trust knowledge (which may include reputation and authorization changes).

5. MIoT App exposes an endpoint to resolve a DID:WEB for its organization application and request it to be registered in the Trusted Organization Registry on the blockchain.

6. The patient has downloaded the SSI Wallet to their mobile and is issued with a Person Verifiable Credential (simulating the EUDIW approach to handle their national eID).

7. The user backs up and encrypts their Person Verifiable Credential (VC) in the mobile wallet to **Credential Recovery** in the case of the need for **recovery** of a lost or corrupted mobile.

Use case postconditions

1. Patient registration and authentication done. Can start using the MIoT kit at home. 2. 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 flows encrypted from the smartphone (MIoT app) to ARCADIAN-IoT services. In these services, an SSI Person Verifiable Credential is presented from the user´s SSI Wallet. 2. Information for hardened encryption is generated at the user mobile device (stored securely in the RoT). Information for verifying user data is securely sent to ARCADIAN-IoT third-party services. 3. User is registered in ARCADIAN-IoT framework by the trusted organization application MIoT, and event raised to inform all framework components. 4. At the authentication step, the MIoT app uses the authentication data from the RoT and of an SSI Wallet. The data is retrieved, and the flow continues from the MIoT smartphone to MIoT services. In these services, the ARCADIAN-IoT authentication process happens with both hardware-based and decentralized credentials and, if successful, information about that is securely returned to the device authorizing the patient to proceed (start the health monitoring).

Implementation details

In the implementation of use case C1, a module has been created within the Medical IoT app that allows users to sign in to access their accounts. Features such as authentication and security measures have been applied to verify user credentials and protect their accounts. Best security practices, such as encryption to safeguard login information and measures to prevent brute force attacks, have been implemented. Clear error messages have also been developed to guide users in case of login issues. No implementation deviations exist.

3.3.3 Use case C2 – MIoT capturing and sending vital signs and perceived health status

Overview

This use case involves monitoring patients with a treatment protocol, collecting vital signs such as heart rate, temperature, SpO2, and blood pressure using medical sensors, and providing timely alerts for medical decision support. The implementation includes the use of a MIoT kit with medical sensors and a smartphone as a gateway and interface for patients to enter perceived well-being. The solution also incorporates a MIoT middleware service for secure data distribution and health alert generation, as well as a monitoring tool for medical staff to check patient well-being, receive alerts, and adjust monitoring protocols as needed.

The main steps of this use case are as follows:

- The patient, at home with sensors synced to the smartphone, runs the MIoT app for health sensor readings and provides perceived health status when necessary.
- The app encrypts the data from the health sensors using Hardened Encryption with RoT - SIM information before sending it to the MIoT services.
- The smartphone sends the encrypted data to the MIoT middleware services, storing it

locally if there is no connectivity, and sending it with a timestamp once communication is restored.

- With patient authorization, the MIoT middleware forwards the data to the hospital for monitoring and decision support by medical staff.

This use case ensures the secure collection, transmission, and monitoring of vital signs and perceived health status for effective patient care and support.

Use case description

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. The main steps are: 1. 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 – **SIM** - 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. 2. 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. 3. With the patient authorization, MIoT middleware forwards the data to the supporting hospital monitoring tools. These third-party tools need to comply with ARCADIAN-IoT[5] 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) – enforced by the **self-aware data privacy** via the **Hardened Encryption** libraries and encryption settings. 5. 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). 6. 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.
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 device behaviour monitoring (and subsequently 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. 4. Remote Attestation attests the device both periodically, and on demand (triggered by the Reputation System), assessing the device's compliance with the requirements to use the service/app.
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), 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., device behaviour monitoring) to infer potential threats and act if needed.

Implementation details

The implementation details of Use Case C2 - MIoT capturing and sending vital signs and perceived health status include the following components and steps:

- Telemedicine modules developed by RGB for monitoring ECG, SpO2, and NIBP with

Bluetooth BLE communication using AES-CCM cipher with 128-bit key length.
- Physiological signal waveform collected by the modules includes SpO2, ECG, and NIBP.
- Measurements derived from the physiological signal include oxygen saturation in arterial blood for SpO2.
- Data used in this use case are user identifiers, authentication material, and data gathered from health sensors.
- The data flow involves encrypting the payload with RoT information and sending it to the MIoT middleware, with the option to store encrypted data in the device if communication is unavailable.
- Implementation steps include integrating the MIoT app with hardened encryption, receiving encrypted data on the web platform, and integrating with Self-aware Data Privacy for data decryption and encryption based on user policies.
- The MIoT app also integrates Remote Attestation for increased trust in smartphone and MIoT service integrity.

3.3.4 Use case C3 – Personal data processing towards alarm triggering

Overview

The Use Case involves the processing of health data in the cloud by the MIoT middleware to detect and trigger health alarm conditions in the hospital monitoring tool. The key aspects of this use case are as follows:

- Encrypted data resulting from Use Case C2 is stored in the MIoT service database for analysis and alert triggering by the MIoT processing unit, which requires registration in ARCADIAN-IoT and patient authorization for data processing.
- Decryption techniques applied by the MIoT processing unit only decrypt the sensor data payload, keeping the patient's identity encrypted and anonymous. Additional data like age, gender, and pathological information may be included in the payload for alarm inference without identifying the individual.
- ARCADIAN-IoT Behaviour Monitoring oversees the MIoT service behaviour, adjusting trustworthiness reputation and authorization based on service performance.
- Alarm conditions detected by the MIoT processing unit are encrypted and merged with the patient's encrypted identification, with patient authorization required for forwarding to hospital monitoring tools.

This use case ensures patient privacy, anonymity, and secure transmission of health alarms to authorized medical staff for monitoring and intervention.

Use case description

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. The key story aspects are:

1. Having the encrypted data that results from C2 in a database of the MIoT service, the processing unit of MIoT wishes to analyse the data and trigger alerts if needed. This MIoT processing unit needs to be registered in ARCADIAN-IoT and the patient needs to authorize the processing of his/her data for this purpose (**self-aware data privacy**). If the patient revokes the grant for processing his/her data, new policies are applied to the encryption of data, so that this unit cannot access the data. 2. 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. 3. ARCADIAN-IoT **device behaviour monitoring**, and subsequently **CTI**, oversee and interpret this MIoT service behaviour, contributing to the adjustment of 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. 4. 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. 5. With the patient authorization, MIoT middleware forwards the encrypted data that includes the alarms to the supporting 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 preconditions
1. Use case C2. 2. ARCADIAN-IoT behaviour monitoring and CTI components monitor the interactions of the devices (and when applicable, 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. 3. Appropriate cryptographic material distributed to the alert processing unit of MIoT.
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 to the processing unit of 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.

Implementation details

The implementation details of this use case involve the following components and processes:

- A module has been created within the web platform that can request the decryption of medical data from the database to check for alerts that need to be shown to doctors or nurses monitoring the patient.
- The encrypted data in the database is sent to the Self-aware data privacy proxy for decryption, ensuring that the module only analyses medical data anonymously to search for alarms.
- Any detected alarms are added to the patient's medical record for viewing by the responsible medical staff.
- The system can generate alerts based on data that falls outside safe limits, such as low saturation measures, and display these alarms for analysis by healthcare professionals.
- The MIoT processing unit analyses health data in the cloud to detect alarm conditions based on medical protocols or health patterns learned from anonymous patient data.
- Alarm conditions are encrypted and merged with the patient's encrypted identification for secure transmission to hospital monitoring tools.

The implementation approach ensures the secure processing and transmission of health alarms triggered by patient data for timely medical intervention and monitoring.

3.3.5 Use case C4 – Monitor a patient and update a patient monitoring protocol

Overview

The use case outlines a scenario within the medical Internet of Things (IoT) domain, focusing on patient monitoring and interaction with medical professionals.

The main goal is efficient and secure patient monitoring at home. Medical professionals authenticate via multi-factor authentication, using Self-Sovereign Identity (SSI) and mobile Network based authentication, to access patient data on the MIoT hospital platform.

Once authenticated, professionals select patients to monitor, potentially viewing multiple patients' data via a dashboard. Patient data remains encrypted in the MioT service database until accessed by an authorized professional, decrypted using ARCADIAN-IoT provided cryptographic keys.

Professionals can edit patient data, which remains encrypted, and send it back to the MIoT app. Patient smartphones must be connected and securely authenticated through ARCADIAN-IoT for command execution.

Medical professionals can adjust monitoring protocols by requesting encrypted changes through MIoT services, ensuring secure communication with patient IoT devices. Successful decryption triggers command execution on the app; otherwise, the request is disregarded.

Use case description

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 use case story with ARCADIAN-IoT participation is: 1. A medical professional authenticates in the MIoT hospital platform with a **strong multi-factor authentication**, where one factor is an Organization Member Verifiable Credential, and another is a mobile Network ID Token. In the authentication flow, these credentials are requested by the ARCADIAN-IoT **MFA** to be validated by their respective **SSI** and the **Network-based Authentication** components and upon successful verification a signed and protected ID Token is returned to the MioT platform by the MFA. 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. Using the ARCADIAN IoT ID token the medical professional obtains private cryptographic keys needed to access the data of the patients that authorized him/her to do so. 2. When successfully logged in, the medical professional selects a patient to whom he/she has authorized access to, based on their authenticated Verifiable Credential, or request access to a new patient. The medical professional can also select 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. 3. Patient's data is kept encrypted until requested by an authorized medical professional. At this moment it is decrypted with cryptographic material provided by ARCADIAN-IoT **hardened encryption** key management component directly for the medical professional. 4. 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, encrypted with **hardened encryption**. 5. Having the necessary authorization, the medical professional using the web interface decrypts the data (with hardened encryption) sent by the patient app. The user edits the intended fields and requests the sending of the new data to the MIoT app. 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. 6. 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 framework as described in Use case C1 – MIoT kit delivery – Patient registration and authentication. 7. When the patient device and the MIoT app receive the encrypted request, the request gets decrypted. 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 preconditions
1. Use case C1. 2. The Medical Professional has downloaded the SSI Wallet to their mobile and is issued with a Person Verifiable Credential (simulating the EUDIW approach to handle their national eID) 3. Medical professional, end user of the MIoT hospital platform has been pre-provisioned in the SSI IdP Issuer with their SSI Person claims matching a medical professional in the Organization´s IdP so that the medical professional can also be issued with an Organization Member VC. 4. Medical Professional issued with an Organization Member VC. 5. MIoT App exposes an endpoint to resolve a DID:WEB for its organization application and request it to be registered in the Trusted Organization Registry on the blockchain. 6. Medical Professional is registered in ARCADIAN-IoT framework as an Organization Member with a mobile Network ID token for a given subscriber for the newly created ARCADIAN-IoT ID. A SIM-based cellular device is needed for this purpose. 7. Medical professional authorized by a patient (or more) to decrypt his health data for well-being monitoring purposes. 8. ARCADIAN-IoT device behaviour monitoring and subsequently CTI components monitor the interactions of the devices (and when applicable, 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. Authorized medical staff is able to monitor patient health data & 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 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 web interface and the medical professional is able to update it. The new commands are encrypted and sent, through the MIoT middleware, to the patient device. At the device, the commands are decrypted 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.

Implementation details

The implementation details involve the following components and processes:

- A module has been created within the web platform that allows doctors or nurses to enter and modify the monitoring protocol for specific patients. The healthcare professional must be authorized to access the patient's data and be included in the patient's encryption policy.
- The web platform displays different views for doctors or nurses authenticating through ARCADIAN-IoT, including a home view showing a list of patients assigned to them, prioritized by patients with unreviewed alerts. The healthcare professional can access the profile of selected patients.
- The patient profile view in the web platform is divided into three pages:
    - The first page displays the patient's personal information and any alarms the patient may have.
    - The second page, related to Use Case C4, shows information on the patient's sessions and allows for modifications to the monitoring protocol, including adding new monitoring protocols and viewing past and upcoming sessions.
    - The third page displays the treatments the patient may have.
- The web platform decrypts the data through the Self-aware data privacy proxy, encrypts it with the Hardened Encryption library, and sends it to the medical staff's browser. In the browser, it is decrypted with the same Hardened Encryption library, shown to the doctor for modifications, re-encrypted, and sent back to the Self-aware data privacy proxy for storage.

The implementation approach ensures efficient and secure monitoring of patients at home, enabling healthcare professionals to update monitoring protocols and make informed decisions based on patient data.

3.3.6 Use case C5 – Patient MIoT devices security or privacy incident

Overview

When under normal usage of the Patient MIoT device, it is subject to a security or privacy incident aimed at accessing or stealing private data regarding the health patient. Potential origins for such incident this include device loss or theft, as well as cyber-attacks (e.g., privilege escalation, Distributed Denial of Service Attacks, NMAP scans, Attempted Encryption of Large Number of Files (Ransomware), Attempted tampering with security token attached to HTTP requests.

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

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). The story related with security or privacy incidents in patient MIoT devices is: 1. 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 **device behaviour monitoring**, **flow monitoring** and later processed 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 dynamically deciding which rules to apply to protect MIoT devices and the IoT network (e.g., from DDoS attacks), based on threat alerts from the device behaviour monitor and CTI and reputation events. 2. For **protecting** the patient's private information, the data collected by the smartphone 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 (**DBM**) and interpreted (**CTI**), as well as **attestation** results. To ensure that no unauthorized control of the sensors happen, only trustworthy smartphones/apps can receive commands that change their behaviour, and these commands can only come from trustable MIoT services. As soon as a smartphone is found to be compromised, the RoT of the device will receive information, from the network, to refuse to provide cryptographic material when requested by the device (RoT has an operating system independent from the device). Moreover, the device communication capacities are kept under control with a network-based **authorization** enforcement tool, which is always aware of all devices' **reputation**. 3. 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 – **SIM**/UICC (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 SSI Wallet). The network credentials manipulation and the **SIM** communication with the network follow the GSMA security accreditation schema.

4. Whenever an **incident is detected by the DBM**, it sends an alert to CTI, DSP, and Reputation System. In turn, the DSP determines the appropriate security policies, and informs the domain owner and the self-recovery about the policies. If possible, the self-recovery applies the policy. In any case, in the "final step" of this process, the DSP sends another message to the **Reputation System** informing it about whether the policies were applied both by the DSP (in this case, saying it was not applied). 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/MIoT app is operational, The MIoT app takes actions for recovery from the incident according to the type (**self-recovery** component). When an incident is detected, the dynamic authorization enforcement component (placed at the network provider core elements) ensures that Self-recovery (recovery of the data) procedure is the only one available to the compromised device until it recovers from the incident. Self-recovery may require access to ARCADIAN-IoT services.

5. If or when the **self-recovery** process is successful, the device is restored to a status of compliance with ARCADIAN-IoT, including credentials recovery. In a recovery scenario, such as a replacement of the mobile device or loss/corruption of credentials, the SSI credentials are recovered from the **Credential Recovery** component.

6. If or when the **Self-Recovery** process is successful, the recovery and restoration of the device to a compliant status with ARCADIAN-IoT is automatic. In case of issues or anomalies that trigger restoration of functionality, data, or configuration to predefined trust levels without manual intervention is made, ensuring continuity of operations and preserving data integrity.

7. When the **Cyber Threat Intelligence** component receives an alert, it will automatically update the information by adding the threat level and category associated with the alert. This updated information is then used to raise an alert for the CSIRT personnel through the GUI interface. Additionally, the IoC (indicators of compromise) identified in the alert is forwarded to other components within the ARCADIAN-IoT framework for further processing and response.

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 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.
3. Remote Attestation performs attestation of the device both periodically and on demand by the Reputation System, whenever necessary, making sure the complies with the requirements to use the service/app.

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, its RoT is informed of this over the air and, from that moment until a successful recovery happens, the RoT will refuse to provide sensitive cryptographic material to the device. 5. In a recovery process, SSI Verifiable Credentials are recovered from Credential Recovery 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.

Implementation details

No additional specific work was necessary from RGB perspective to implement this use case, as all the involved ARCADIAN-IoT components were integrated in the scope of previous use cases. The execution of C5 builds on previously performed integration with Device Behaviour Monitor and Self-Protection to monitor and mitigate threats, and a Remote Attestation mechanism that uses RabbitMQ for securing communications and maintaining device integrity. It integrates patient and doctor credential recovery through ATOS, works with 1GLOBAL for reputation-based communication authorization enforcement, and employs a robust encryption module co-developed by XLAB and 1GLOBAL for protected medical communications. The system is built to be adaptable, proactive, and secure, with continuous improvements such as latest Martel proxy update to improve performance. UWS has implemented a 5G security system with three components: network monitoring for threats, analysing and planning of a mitigation response, and then implementing protection measures, all communicated through RabbitMQ, ensuring quick and coordinated defence against known cyber threats like DDoS attacks.

3.3.7 Use case C6 – MIoT cloud services security or privacy incident

Overview

This use case revolves around incident response within the healthcare sector, involving network infrastructure, as well as the cloud services responsible for user authentication in medical devices. Its primary objective is the full detection, planning, and mitigation of incoming threats.

When under normal usage of the Patient MIoT device, the MIoT Cloud Service is subject to a security or privacy incident, such as a Distributed Denial of Service (DDoS) attack coordinated via a botnet.

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

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 to MIoT Cloud services (e.g., the data processing module for health alarm triggering). It includes the preparation of the services (for incident **detection** and **recovery**), the private data and identity **protection** and the subsequent actions of **recovery** and **healing**. The security incident focused on this use case scenario is a DDoS attack orchestrated in a botnet combined by infected MIoT devices and internet devices, with the target on the MIoT Cloud Services. The story related to this use case is: 1. To effectively detect, protect, and recover from security or privacy incidents, each MIoT Cloud service must integrate with ARCADIAN-IoT components. During this process, information is securely collected by framework components such as **Device Behaviour Monitoring** and **Network Flow Monitoring** and then interpreted by the **Cyber Threat Intelligence** system. 2. Additionally, the **Network Self-protection** component will be in place to deduce threats by analysing data received from sources like **Network Flow Monitoring**, and by applying 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). To protect the patients' private information, the service is only able to decrypt the part of the payloads that have the health data. Apart from that, the service deals with anonymised 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. 3. Also, for protection and triggering incident mitigation measures, the ARCADIAN-IoT dynamic **Reputation System** defines the trustworthiness of the compliant service according to several factors, including their behaviour and data flow, which is being monitored and interpreted (**CTI** and **Network Self-protection**). 4. In the case of a security incident being detected, the **Reputation System** is updated immediately, as well as the authorization enforcement's accesses. Hence, 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 **Network Self-healing** components). The Self-recovery component focuses on the recovery of the data and the **Network Self-healing** focuses on the recovery of the system functionalities. 5. If or when the self-recovery and **Network 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 **Permissioned Blockchain** component. Human intervention is reduced to the strictly necessary in healing and recovery procedures. 6. To protect the business continuity of the services, the **Network 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. 7. When the **Cyber Threat Intelligence** component receives an alert, it will automatically update the information by adding the threat level and category associated with the alert. This updated information is then used to raise an alert for the CSIRT personnel through the GUI interface. Additionally, the IoC (indicators of compromise) identified in the alert is forwarded to other components within the ARCADIAN-IoT framework for further

processing and response.
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 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 nonhuman 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.

Implementation details

No additional specific work was necessary from RGB perspective to implement this use case, as all the involved ARCADIAN-IoT components were integrated in the scope of previous use cases, namely:

- To effectively detect, protect, and recover from security or privacy incidents, each MIoT Cloud service integrates with ARCADIAN-IoT components, including Device Behaviour Monitoring, Network Flow Monitoring, Cyber Threat Intelligence system, and Network Self-protection component.
- The MIoT services involved in this use case need to decrypt patients' private data for incident mitigation measures, but they only decrypt the part of the payloads containing health data, maintaining anonymized patient identity without access to cryptographic material for decryption.
- ARCADIAN-IoT components, such as Network Self-protection, analyze data from sources like Network Flow Monitoring to deduce threats and apply intent-based protection rules dynamically to protect services from threats like DDoS attacks.

The implementation approach highlights the measures taken to address security or privacy incidents in MIoT Cloud services, ensuring the protection of private data, identity, and the overall security of the system.

3.3.8 Use case C7 – Medical 3rd party security or privacy incident

Overview

In C7, when under normal operation 3rd party medical services, they are subject to a security or privacy cyber incident (e.g. Privilege escalation, Distributed Denial of Service Attacks, attempted tampering with security token attached to HTTP requests).

Further details are provided in the use case story and the validation scenarios chapter.

Use case description

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). The story related with this use case is: 1. 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 **device behaviour monitoring** and **flow monitoring,** and interpreted by a **cyber threat intelligence** tool.

2. 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. 3. 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**). 4. 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. 5. 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. 6. 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. 7. 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. 8. When the **Cyber Threat Intelligence** tool receives an alert, it will automatically update the information by adding the threat level and category associated with the alert. This updated information is then used to raise an alert for the CSIRT personnel through the GUI interface. Additionally, the IoC (indicators of compromise) identified in the alert is forwarded to other components within the ARCADIAN-IoT framework for further processing and response.
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 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., device 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 no 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.

Implementation details

No additional specific work was necessary from RGB perspective to implement this use case, as all the involved ARCADIAN-IoT components were integrated in the scope of previous use cases.

Use case C7 leverages ARCADIAN-IoT for mitigating security threats and ensuring the protection of third-party services that are integral to the medical application domain, such as the web browser used by the doctor/nurse while viewing patient medical data over 5G connections.

4. USE CASES TECHNICAL VALIDATION

This section presents the pursued technical validation scenarios of the different use cases across the three ARCADIAN-IoT pilot domains (A: Emergency and vigilance using drones and IoT, B: Grid Infrastructure Monitoring, and C: Medical IoT). The performed validations, aimed to verify the extent to which the ambitioned innovations have been reached, represent the main outcome of the validation task (T5.5). Given the multidisciplinary nature of the activities, spanning both technical, ethical and legal aspects, all consortium partners have been involved: technical partners, (application) domain owners and legal experts (the legal validation is presented in section 6). The validation steps listed in the following sections have been executed, and the associated evidence has been collected and processed. Such evidence is confidential and documented in the final report [11].

It is important to highlight that, for some validation scenarios, the component's involvement is a subset of the component's involvement defined during the integration stage (depicted in the integration plan - Figure 9). This is justified by the following reasons: 1) the validation (or collection of evidence) of some the component's involvement in the validation scenario doesn't further contribute to verifying any of the defined KPIs; 2) some components have a passive role in specific use cases where they are involved (e.g., Device Behaviour Monitoring in Validation Scenario A3#1).

4.1 DOMAIN A – Emergency and vigilance using drones and IoT

4.1.1 Use case A1 – Person Registration at DGA service

Validation scenarios overview

A1 use case was validated using a single validation scenario focusing the person registration in the DGA service via 3 authentication factors (Biometrics, DID, network credentials).

Validation scenario A1#1 description

Prerequisite conditions:

- An Android smartphone with a camera and a SIM is available (provided by 1GLOBAL).
- The SIM has installed 1GLOBAL's security applets and the DGA app SHA1 signature for being authorized to use its functionalities. The SIM security applet middleware is integrated with the DGA app (within the Hardened Encryption component)
- The device is configured to use an ARCADIAN-IoT private APN (private cellular network) for testing the network-based Authentication and Authorization components.
- DGA App is downloaded and installed on the mobile device.
- The SSI Wallet App is downloaded and installed on the mobile device.
- The organization service is registered in the ARCADIAN-IoT Trusted Organization Registry with its Decentralized Identifier (DID: WEB) so that any person or device registrations to the ARCADIAN-IoT framework is validated by the associated DIDs signing key.
- The organization service provides a DID: WEB endpoint used for making its public signing key available.
- Evidence appraisal policy and reference values have been transmitted from the DGA service to the Verifier, for enabling the smartphone to be attested.

The following actions are required for the validation:

1. User opens DGA App, inserts requested data & clicks on buttons to Registration Click on

link to be issued with a mobile wallet identity, and user resultantly receives an identity in their SSI Wallet.

2. Now that the user has a wallet identity, they proceed to register for the service by clicking on register in the DGA app.
    a. The mobile app calls a URL to the ARCADIAN-IoT Framework which is redirected to the SSI IdP.
    b. The user receives a request on the mobile app to present their Person Verifiable Credential that was previously issued to them.
    c. The user confirms the presented credentials, and an ID Token is created for this user.
3. The DGA app, which is authorized to communicate with the SIM (the SIM has its SHA1 signature for authorization), requests a new key pair generation in the SIM, through the Hardened Encryption library. These keys will be used for a Root of Trust (SIM) digitally signature flow. Upon request of the key pair generation, the SIM returns the public key to the requesting Hardened Encryption method. The public key is sent to ARCADIAN-IoT key management system, for future validation of SIM digital signatures. The private key, which should be used to sign outgoing encrypted payloads, is stored in the SIM secure element.
4. User is asked to confirm its identity on the DGA app and click to continue with the registration and create an identity in ARCADIAN-IoT framework. Thus, a registration request is sent to the ARCADIAN-IoT framework with the ID Token and the mobile network token, which is signed by the DID associated to the registered trusted organization service.
5. The ARCADIAN-IoT framework validates the registration request that is signed by a trusted organization registered in the framework´s Trusted Organization Registry and creates a new aiotID if successful and is not previously registered.
6. User is next asked to provide photo images to complete the registration for this new aiotID and the user provides their images as requested by the app. All personal data is encrypted and signed by the RoT using the HE component.
7. User is informed on the DGA app that their registration is complete.
8. Registration event is sent to the ARCADIAN-IoT Framework with their Person Identity and associated aiotID.
9. ARCADIAN-IoT Framework services (Reputation, Network-based Authentication and Authorisation, Device Behaviour Monitoring) initialise their respective services for the new aiotID.
10. Reputation System sends an Attestation Cue, both informing the Remote Attestation about the smartphone's aiotID and triggering its attestation.

4.1.2 Use case A2 – Person authentication at the DGA service

Validation scenarios overview

A2 use case was validated using a single validation scenario focusing the person authentication in the DGA service via 3 authentication factors.

Validation scenario A2#1 description

The use case focuses on a person, particularly a DGA user, authenticating in DGA services using ARCADIAN-IoT multi-factor authentication (MFA). This process, integrated within the DGA solution, will allow to validate the following ARCADIAN-IoT components: (1) MFA; (2) hardware-based identification and authentication (network-based); (3) Biometrics; and (4) the Self-Sovereign Identity (SSI) / Verifiable Credentials (VC).

The expected result is to have a person authenticated using the three authentication factors.

The following actions are required for the validation:

1. Using the DGA app to authenticate, the person is requested to take a photo. The photo is sent to the DGA backend in a secure way, appended to the ARCADIAN-IoT ID to use to authenticate, and using the Hardened Encryption. The Hardened Encryption action shall consist of securing the photo with the key generated and stored on the permissioned blockchain.
2. Communicating through the cellular networks, when the request passes through the core network infrastructure, ARCADIAN-IoT Notarizer appends to the authentication request a signed and protected Network ID token (transparent to the user).
3. The person authentication request reaches the DGA backend services, which forwards the request to the MFA component.
4. The MFA splits the request received, asking: (1) ARCADIAN-IoT's Biometrics component to confirm whether the photo received matches that ARCADIAN-IoT ID; (2) the Network-based authentication component to confirm if the Network ID token issued by the core network is valid and matches that ARCADIAN-IoT ID; (3) and the SSI component to validate the identity of that ARCADIAN-IoT ID.
5. The Biometrics and the Network-based authentication components validate the received identifiers for that particular ARCADIAN-IoT ID and answer to the MFA with the result.
6. The SSI component establishes a secure communication with the SSI Wallet in the personal device to perform the verification of the person identity. The result is also sent to the MFA.
7. As the three authentication factors verification were positive (the three different identifiers correspond to the intended ARCADIAN-IoT ID) the MFA issues and signs an ARCADIAN-IoT ID Token and returns it to the DGA backend. Next returns it to the requesting personal device – the person is now authenticated and can proceed with the use of the DGA mobile app.
8. MFA also shares the results of the authentication events with other ARCADIAN-IoT components. This information is used by the Reputation System to update the reputation of the involved entities - persons.

4.1.3 Use case A3 – Person retrieving and editing personal data

Validation scenarios overview

The use case focuses on a person/user editing the personal data through the DGA App, using only one scenario.

Validation scenario A3#1 description

The use case focuses on a person, particularly a DGA user, retrieving and editing its data in the DGA service. This use case will allow to validate the following ARCADIAN-IoT components: (1) Behaviour monitoring; (2) Biometrics; (3) Hardened Encryption; (4) Authorization, (5) Reputation System and (6) Remote Attestation.

Prerequisite conditions:

- The Domain Owner / IoT Service Provider has previously sent Reference values for being used by the (Remote Attestation) Verifier for appraisal of a device's evidence.
- The person has a smartphone with the DGA app installed, the SSI Wallet and has already authenticated, as per the A2 use case.

The following actions are required for the validation:

1. Using the DGA App, the person supplies personal data to the DGA service, which includes name, address, photo, and optional SOS contacts.
2. The DGA service, can use the reputation information of the user and device, before

providing the requested data to the user.
3. Upon the reputation values, according to the configured policies, the data is retrieved to the personal device of the user in an encrypted way.
4. On the personal device, with the DGA app, the data is decrypted using the ABE key through the hardened encryption component. The user edits its personal information on the personal device, and after the confirmation of the use, the DGA app sends the modified information to the DGA service in an encrypted process. This encryption process requires the use of ABE keys, which are managed by the Hardened Encryption. As the user edits its photo on the personal device, there is an interaction with the biometrics component to identify the user. Partial steps of the Use case A2 can occur. On the user confirmation, the DGA sends in an encrypted fashion the data with the DGA service.
5. The Remote Attestation procedure is successfully performed:
    a. The procedure is initiated via a manual trigger at the Verifier (running at a remote server)
    b. The attester (running in the smartphone) receives the associated attestation request (challenge) sent by the Verifier, collects the requested claims (dummy data at this stage), processes them (i.e. encapsulates them as Evidence) and sends the response to the Verifier.
    c. The Verifier displays the received Evidence, which should correspond to the claims displayed at the smartphone side.

Recall that this use case focuses on a person, particularly a DGA user, retrieving and editing its data in the DGA service. This use case will allow to validate the following ARCADIAN-IoT components: (1) Behaviour monitoring; (2) Biometrics; (3) Hardened Encryption; (4) Authorization, (5) Reputation System and (6) Remote Attestation.

4.1.4 Use case A4 – Person Requesting a DGA Service

Validation scenarios overview

The use case focuses on a person, particularly a DGA user, requesting a DGA service, using only one scenario.

Validation scenario A4#1 description

These following actions are required for the validation

1. Using the DGA app, the person requests a service in the user's location to the DGA Service, sending the necessary personal data encrypted with RoT information: location and an image of the face in the current conditions.
2. The reputation system verifies the user's identity, location and the requesting app and device trustworthiness.
3. Upon the reputable reputation values, according to the configured policies, DGA service will select a drone from the available ones considering the IoT device reputation. Drones' reputation can be formed considering factors like known vulnerabilities or dynamic knowledge built by ARCADIAN-IoT's behaviour monitoring and cyberthreat intelligence components.
4. The integrity data of the drone is retrieved and attested, assuring the device and the DGA service trustworthiness.
5. DGA Service shares the necessary data (location), encrypted, with the drone.
6. The device decrypts the data, obtaining the location of the user.

7. The person is informed through the DGA app that a trustworthy drone has its location and identification for performing the service (self-aware data privacy). Drone's identification may be shared with DGA service's consumer when relevant, for a visual identification upon the devices' arrival to the service location.
8. The DGA service provides the basic information to start receiving video stream from the drone and identify the person that requested the service. The information is composed by URL video stream and the person identifier.

The result of scenario A4 is to have a trustworthy drone with the location of the user that has requested the service using the DGA app.

4.1.5 Use case A5 – DGA Service

Validation scenarios overview

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.

Validation scenario A5#1 description

The validation scenario is the following:

1. The drone **moves to the locatio**n of the requested service.
2. **Once at the given position**, the drone informs ARCADIAN-IoT DGA services that it has arrived the location of the service.
3. ARCADIAN-IoT DGA services inform the person, via the mobile App, that the drone has arrived, what is the device security and privacy reputation, and that he/she should get closer to it and allow **biometric identification**.
4. The person moves **to the service location,** and, on its arrival, a process of **biometric authentication** mediated by ARCADIAN-IoT DGA services takes place. All the private data is securely exchanged.
5. The drone starts the **biometric identification**. For that, it shall start streaming video to the DGA service securely. This data is only accessible by DGA services authorized by the user.
6. When the DGA facial recognition service identifies the user, a **confirmation message** is sent to the backend DGA services, and from then to the drone and **to the user**. The user can then start walking.
7. If the person, **personal device or app recognition fails** (after 120 seconds), the drone informs ARCADIAN-IoT DGA services and returns to the base. Such events, as well as the successful ones, feed the digital reputation of the user, personal device and/or drone through the behaviour monitoring component.
8. If the **process of identification is successful, the drone follows the user** and, if something abnormal (e.g., physical threat, user's injury) is detected, data about the event is collected, encrypted with RoT information, and sent to DGA services.
9. In DGA services, the event data **is decrypted for being analysed by an operator**, who performs the follow-up measures needed.
10. The service ends when the user informs, using the app, DGA services that it has arrived to the desired location and that the drone service is no longer needed. At the end of the service, 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 for his privacy related self-awareness and may choose to delete it.

4.1.6 Use case A6 – Drone security or privacy incident

Validation scenarios overview

In this incident, an attacker launches a privilege escalation attack to compromise and take control of the drone. The attack is detected by the Device Behaviour Monitoring component which triggers a sequence of response (e.g., device attestation and reputation update) and device recovery actions from ARCADIAN-IoT framework, as described below.

Validation Scenario A6#1 description

The validation scenario is broken down into 2 stages:

Attack & response stage:

1. Launch a privilege escalation attack followed by a simulated brute force attack within the device.
2. The DBM detects the attack.
3. The DBM sends an alert to RabbitMQ exchange to alert subscribed components (reputation system and CTI).
4. The CTI[4] component receives the alert. It converts the alert into MISP format and enriches it by adding threat level and class details to provide a better understanding of the potential threat. It then displays a warning message to alert the system operators or security analysts about the potential issue. Additionally, it sends an Indicator of Compromise (IoC) to the framework buffer to ensure that appropriate actions can be taken to mitigate the threat.
5. DSP, upon receiving an alert from the DBM, determines the relevant policy and sends this information for self-recovery, to determine whether it something can be done. The self-recovery in turn returns a message confirming if the policy was applied or not.
6. Reputation system receives the alert (including IoCs) and updates the reputation accordingly.
7. Upon receiving the attack alert, reputation system also requests the change of the communication policy from the Network-based Authorization. This component automatically blocks the communication and thus blocks the attack intention (e.g., data leakage or unauthorized access to the device). Furthermore, the Network-based authorization informs the SIM about the device level of compromise. With this information, the SIM security applet stops providing digital signatures (In the Hardened Encryption normal flow), ensuring that any communication done using other means (e.g., WIFI) is not trusted (avoiding this data poisoning or impersonation).
8. Drone backend application detects this event on the framework and confirms that the Drone is not reachable anymore.
9. Reputation System determines that the trust level of the IoT Device is 0 and publishes this security event on the ARCADIAN-IOT Framework.
10. 3rd Party entity responsible for security governance of Drones (e.g. national body), audits the drone and observes the reputation score downgraded to 0. As no such 3rd party entity is in the project this will be simulated.

Recovery stage, taking place only in case the drone is physically recovered by DGA

[4] The CTI system is pre-loaded with ML models. While their evaluation was done in WP3, the training of the event classification module, which includes features from the Federated AI component, underwent separate validation for its demonstration. A description of this validation involving three distributed entities is provided in Appendix D.

service owner:

11. The DGA notifies the reputation system that the drone is ready to start the recovery process.
12. The reputation system processes the DGA notification, increases the reputation of the IoT device, and requests a change in the communication policy from the Network-based Authorization.
13. The Network Based Authentication Enforcement (NBAE) restores the communication and informs the SIM that digital signatures should remain disabled.
14. Upon detecting that the IoT Device can now communicate through the network, the DGA services shall now:
    a. Request drone's re-onboarding and so recovering its previous DID and Verifiable Credential Recovery to the drone´s SSI Agent.
    b. Order data recovery from Self-recovery.
    c. Notify the reputation system that the drone has been recovered and re-onboarded
15. The reputation system processes the DGA notification and sends a communication policy request to the NBAE.
16. The NBAE component resumes the signing of payloads and sends a notification back to the reputation system.
17. The reputation system processes the NBAE notification and requests a remote attestation to the Drone
18. The remote attestation procedure takes place, and the reputation system receives the attestation result.
19. The reputation system processes the attestation result; as it fulfils its policies the reputation of the device is increased.
20. The DGA backend verifies the payload and the payload signature, upon successful verification the App continues the with further data transfer.
21. 3rd party entity accesses the Blockchain to monitor all security events raised by the drone and can see that the reputation has been restored within acceptable levels.

4.1.7 Use case A7 – Personal device security or privacy incident

Validation scenarios overview

A7 use case was validated using two scenarios, A7#1 and A7#2. In the first scenario the attacker targets the communication between the devices and backend, while in the second scenario the attacker targets directly the mobile device. Further details are given in the individual scenario descriptions.

Validation scenario A7#1 description

Name: Remote attestation incident

In this incident, an attacker intends to deprive the device of communication with its backend or related services. For this reason, the attacker gains unauthorized access to the device and intends to induce a replay attack. This requires the device to send a message with a nonce that was previously used, triggering a chain of events that might trigger changes in the device's reputation and protection measures.

Scenario:

1. A malicious actor gains access to the device with an undetectable approach.
2. The device undergoes the expected attestation procedure. In this case, security incident, action b) takes place.
    a. Under normal circumstances, the attestation returns a JSON to the reputation system with the portion of claims (i.e., how many of the total claims have been

correctly verified against the reference values), the aiot-id and the time stamp of message generation.

b. In the event of a security incident within the attestation process (in this case, a replay attack), the attestation procedure returns a JSON to the reputation system with the respective changes in the JSON (indicating that a problem occurred in the attestation of the device)

3. The reputation system receives the attestation response from the verifier (a sub-component of the remote attestation component).
4. The reputation system receives the information and reduces the device's reputation accordingly.
5. Reputation system publishes the reduced reputation to the Blockchain for its associated ARCADIAN-IoT ID.
6. 3rd Party entity responsible for security governance of Drones (e.g., national body), audits the device and observes the reputation score downgraded. As, no such 3rd party entity is in the project this will be simulated.

Response:

7. To mitigate the attack, the reputation system requests the NBAE component to propagate the trust information to the SIM. In this case, it is taken into account that the device has several apps, and the mitigation action should just target the DGA app. Therefore, no new trust-based cellular network authorization policy is created as the ones existent in ARCADIAN-IoT would affect the whole device and not a specific app.
8. The NBAE informs the SIM/eSIM located at the device that its host is compromised.
9. With this information, the SIM security applet stops signing the payloads that are encrypted by the Hardened Encryption component (the sensitive information that is signed by the SIM). With this action the receivers of the payload are informed that it came from a compromised device, being able to discard it.

Recovery:

10. Domain owner takes action on the affected app (i.e., software update or internal backend check).
11. After action is taken, the DGA notifies the reputation system that the app has been updated or that the internal backend check was successful).

Validation scenario A7#2 description

Name: Verified Credential

Scenario: This scenario is where the mobile device was hacked and all data on the mobile was corrupted or lost and is then recovered.

Mitigation: The user is recommended to perform a factory reset and re-install the SSI Wallet and recover their previously issued credentials.

The following steps are followed to validate this scenarios:

1. The Verifiable Credential is backed up in the wallet app by the SSI Broker.
2. The user can enter in settings and delete all the wallet app.
3. The user selects the mobile wallet app again, and provides fingerprint authentication in order to gain access to the wallet app.
4. The user then proceeds to restore the wallet credentials, by entering in email and password.
5. The user selects the DGA app which requests a new wallet connection as part of the recovery, for its registered email. This must be accepted on the mobile wallet app. It then continues with the recovery process by performing a re-registration. If the identity has

been previously registered a 409 conflict error code will be returned with the associated aiotID.

6. The user then requests the DGA app authentication for the aiotID and is successfully logged in after the user presents the VC from the wallet app, succeeds in face authentication and the smartphone authenticates in the mobile network.
7. The user can request any backed up data in self-recovery to be restored also to the DGA app.

4.2 DOMAIN B – Grid Infrastructure Monitoring

4.2.1 Use case B1 – New Device Registration

Validation scenarios overview

Validation of scenario B1 is done by registering a GMS IoT device into the Hardened Encryption System and into the other security systems (Reputation System, Device Behaviour Monitoring, Remote Attestation, Self-aware Data Privacy).

Validation scenario B1#1 description

1. The vendor-authorised operator logs into the device firmware, using his unique user credentials, leading to the provisioning of the following information:

- A unique (per fleet) Device ID, user and password.

- APN name, user and password, according to what has been provided by the mobile operator supplying the SIM subscription.

- DIDs.

- The accepted attestation claims (i.e., Reference Values), considering the device characteristics, towards the Remote Attestation Verifier, according to defined policy.

2. Login is performed into crypto chip firmware using Root of Trust vendor tool, and via unique credentials. Keys (pre-generated by vendor's tool) are provisioned for all communication stages, into the device encryption repository.

3. The vendor-authorised operator authenticates in the GMS Middleware platform, using his unique user credentials, where the following are provisioned:

- The Device ID and its keys (previously defined into device encryption repository).

- The API interface with the IoT platform - to which data will be forwarded and from which commands will be received. The API uses a unique key and credentials provided by IoT platform vendor[5].

4. The API interface with Remote Attestation (Verifier) is configured.

5. The Rabbit MQ interface with the other security systems connected to Middleware is configured (Reputation, Device Behaviour Monitoring, Self-Aware Data Privacy, Decentralized Identifiers Authentication).

6. A grid infrastructure manager / authorised user authenticates in the IoT platform with a 2-factor authentication and credentials – the lack of any of these 2 authentication factors will not permit the login. The Device ID, its connected sensors and set of data relevant for Grid operations are provisioned. The API interface with GMS Middleware is configured.

7. The GMS IoT devices policy and each new registered Device ID are defined into Reputation System. It is defined into Remote Attestation Verifier the claim and registered each new Device ID configured. Each new configured Device ID is registered into 1) Device Behaviour Monitoring 2) Self Aware Data Privacy, 3) Decentralised Identifier Authentication System, along with the

[5] If there are multiple IoT platforms connected to the Middleware, each will use a dedicated and unique interface

associated DID[6].

4.2.2 Use case B2 – GMS IoT device data gathering and transmission process

Validation scenarios overview

Validation of B2 scenario is done by running independently the GMS IoT device to gather data from local field sensors connected to it, processing, encrypting, and transmitting this collected data, via Hardened Encryption System, to the IoT platform responsible for customer data management.

Validation scenario B2#1 description

1. After reboot, Device authenticates via the Network Authorisation, by IMSI. Device obtains a data bearer, by authenticating into Mobile Broadband subscribed service, with APN user and password provided by operator.

2. Once data bearer (channel) is opened, Device sends a message to the Middleware, by encapsulating ID, user, password, encrypted with key assigned for authentication stage. Middleware decrypts the message and authenticates the Device. If any of provided info is wrong, Middleware bans the authentication, and informs the Reputation System, which will decrease the reputation score (this is more detailed described into B4 use case).

3. Middleware informs IoT platform connected to it, via an API implemented for such task, and this one does its own dedicated authentication process, too. This one is independent of HES but recommended for each IoT platform consuming the sensors data / sending commands to GMS IoT devices.

4. Device activates the sensors data gathering agent (a firmware module), runs as it was preprogrammed the data collection, applies for data post processing the edge agent (another firmware module), encrypts with key assigned for traffic stage, and sends the data to Middleware. Middleware decrypts the message and validates the Device traffic. If the key used is correct and correspondent to that Device ID and stage. If the correspondent key is wrong, Middleware bans the traffic, and informs the Reputation System, which will decrease the reputation score (this is more detailed described into B4 use case).

5. Middleware forwards to IoT platform connected to it, by API for such scope, and using TLS encryption of traffic message, and the IoT platform, once decrypt properly, runs the data management of field sensors where from it was gathered.

6. Device Behaviour Monitoring system subscribes the exchange that provides device events and monitors the devices behaviour.

4.2.3 Use case B3 – Service request from third-party IoT monitoring platform

Validation scenarios overview

Validation is done by permitting to the appointed users (via role playing) the execution of tasks, with final scope of successful command execution, from IoT platform to GMS IoT devices, through Hardened Encryption System.

For R&D reporting accuracy, KPI of total time necessary to perform a command using Hardened Encryption System, could be influenced by:

[6]There was no signed registration validation against the organization service DID in the Trusted Organization Registry. This has been a late change, which could not be accommodated in time, requiring extensive architecture and coding changes.

- setup frequency of “spectrum” reading for each GMS IoT Device;
- type of telecommunication technology (protocol, spectrum access technology, frequency);
- integration into same Docker or into different Dockers of IoT platform and Middleware;
- integration into Dockers hosted by different cloud services providers (e.g. Docker 1 – containing the IoT platform – running into AWS, and Docker 2 – containing Middleware – running into Azure);
- internet QoS (including firewall implementation specific policies and gear running that) of each cloud provider involved;
- computing power of hosting infrastructure.

Validation scenario B3#1 description

1. A grid infrastructure manager / authorised user authenticates in the IoT platform with a compliant 2-factor authentication and credentials. Missing of any of these 2 steps will not permit the login.
2. Successful login will give access to the user to the devices registered into its authority. Devices part of access policy is visible into IoT platform front end dedicated page.
3. When successfully logged in, the user selects from specific IoT platform device front end page (“Devices”) a GMS IoT device (from the grid infrastructure he has access to). User selects “OTA” front end page / submenu, then selects “Send OTA command”, choose the port and type of command by fulfilling the value (“value” is correlated with Device firmware ports specific), and performs “Submit” action.
4. IoT platform communicates with Middleware through an API, which of interface was defined previously.
5. Once Middleware receives the command, decrypts it (by TLS decryption). It sends the IoT traffic (command) to Hardened Encryption System.
6. Hardened Encryption System (Middleware component) identifies into its data base the key assigned for that Device ID where command must be sent. It does the encryption of the IoT traffic (command) with this key. It sends the encrypted string to GMS IoT device.
7. GMS IoT device has set-up into firmware configuration a time frequency when it listens the received traffic. Just the traffic with its Device ID will be considered. When new traffic is received, the GMS IoT device master firmware will engage the Hardened Encryption System agent (which is a worker firmware called by main firmware), and this one will check if the key used to encrypt the traffic from IoT demanding platform was using the similar key provisioned into crypto chip repository. If so, the decryption (provided by RoT of crypto chip) will run, and command will be locally interpreted by other firmware agent (in charge with local control of ports). If not, the decryption will fail, command will not be executed.
8. Device will notify any of these events to Device Behaviour Monitoring system (publishing to the DBM queue with this specific incident) and Reputation system (providing the value agreed into policy).
9. Independently of the command execution, GMS IoT device checks the status of local control port actuated / status changed and triggers a B2 scenario (scope being to inform the IoT platform and its authorized users, for record tracking purposes and accurate infrastructure control).

4.2.4 Use case B4 – GMS IoT device security or privacy incident

Validation scenarios overview

Validation of B4 scenario is done by permitting to the appointed users (via role playing) the execution of tasks, with final scope of **unsuccessful** authentication, sensors data transmission to

IoT platform, or command execution, from IoT platform to GMS IoT devices, through Hardened Encryption System.

Each validation was followed by a recovery to be demonstrate that the Device Behaviour Monitoring works continuously, despite changes occurred challenging the security of these. This use case stresses indirectly the Reputation System, too.

Validation scenario B4#1 description

1. Device keys are provisioned correctly, same with Middleware hardened encryption data base. It is performed the local login to device hardware, by specialised provisioning hardware kit. It is used the software application provided by crypto chip supplier, to access the keys repository. It is changed the key correspondent to Device ID authentication, with a new one. It is performed the logout. Device is rebooted.
2. Device will connect to the data network. Then it tries to authenticate to the Middleware. Middleware does not recognize that key as being assigned to that Device ID. It rejects the authentication.
3. Middleware publishes on Rabbit MQ the unsuccessfully trial.
4. Device Behaviour Monitoring instance consumes the message (and could proceed further actions such as issuing an IoC to the CTI).
5. Reputation System consumes the message, identify the message type vs. defined claim, and downgrades the reputation of that Device ID, for that stage of lifecycle.
6. Step 1 is repeated, this time the DiDs are changed with others which are not defined into Decentralised Authentication system.
7. Device successfully authenticates into Middleware (keys were not touched, this time), but then after sends to Decentralised Authentication system the correspondent information. This one rejects the authentication, informs the Middleware, which blocks the Device to close its authentication process. At the same time, Device Behaviour Monitoring consumes from RabbitMQ the failure message and its details (Device ID, stage); Remote Attestation consumes the same message, identifies the message type vs. defined claim, and downgrades the reputation of that Device ID. No traffic (sensors messages sent to IoT platform, commands sent from IoT platform) are possible anymore with this Device ID, until incident is not solved and a proper recovery (authorized, case by case, in real live operations, by Grid responsible operator / representative) is done. Example of recovery could be rewritten of new DiDs for that Device ID (which is part of use case B1).
8. Step 1 is repeated, but this time it is changed the key correspondent to Device ID traffic (sensors data transmission to IoT platform), with a new one.
9. When device sends a new set of data from sensors, it encrypts this with the correspondent (but wrong) traffic assigned key. Middleware will not decrypt this message, so will refuse to relay the (not accessed) content forward through API to IoT platform. Steps 3., 4. & 5. described above are repeated.
10. Then, to simulate an incident on device, but not triggered by an attack on device, this time it is changed the key correspondent to Device ID commands (sent by IoT platform, for being executed locally), with a new one, into Middleware Hardened Encryption data base.
11. When device gets the command, it fails the decryption of the command, so will not execute something which is not understood (and processed by firmware module dedicated for local commands translation to hardware ports). Device informs the Middleware about the failure. Steps 3., 4. & 5. described above are repeated.

4.2.5 Use case B5 – GMS middleware security or privacy incident

Validation scenarios overview

Validation of B5 scenario is done by permitting to the appointed users (via role playing) the execution of tasks, with final scope of **unsuccessful** API connection, between Middleware and IoT platform, and of **unsuccessful** login to Middleware.

In case of API unsuccessfully connection, it was checked into IoT platform side for the same purpose, and evidence was collected.

Validation scenario B5#1 description

1. Middleware API credentials are correctly defined in both end points (IoT platform and Middleware). It is performed a login to IoT platform. It is disabled the API interface.
2. Middleware tries to connect and fails.
3. Middleware publishes on Rabbit MQ the unsuccessfully trial.
4. Reputation system consumes the message and updates the Middleware reputation score. Devices could authenticate, but cannot perform traffic or get commands, these being end-pointed to IoT platform.
5. After reenabling the interface, Middleware successfully connects to IoT platform. After this, once API service is restored, devices can transmit again sensors' data, and/or receive commands from IoT platform, through Middleware, if all the other authentication & traffic conditions (keys, DiDs, etc. are respected).
6. Middleware publishes on Rabbit MQ the successfully trial. Steps 3, 5 and 6 run again, continuously, for each API status change.
7. Reputation System consumes the message and updates the reputation score if login to Middleware is not done accordingly (wrong credentials, wrong 2-factor numerical code), these events could be notified too.

4.2.6 Use case B6 – External data audit to grid infrastructure

Validation scenarios overview

Validation of B6 scenario is done by permitting to the appointed users (via role playing) the execution of tasks, with final scope of successful logins (if the credential info used is correct), data recovery (local copy on a device), configuration removals, and offline notifications required by the process.

Validation scenario B6#1 description

1. Upon request from an Authority agent, the GMS technology vendor provides an auditing hardware kit which supports the local login process on the GMS IoT device.
2. Kit is connected to the GMS IoT device, by vendor representative, in presence of grid and Authority representative.
3. Vendor representative logins to GMS IoT device, by using its firmware configuration software tool. It he does not use the proper credentials, access is refused.
4. Grid representative, using GMS IoT (same, as used above) computer, logins to Middleware, by using its configuration front end dedicated section. It is selected the Device in scope of Authority investigation. It is selected the "Encryption" menu section. It is copied the encryption key defined for this B6 use case specifically (ID of key is part of convention with customer, before B1 provisioning; usually it is ID#6).

5. Vendor representative uses the key to decrypt the stored information. Extracted file, decrypted, is saved locally to a memory support provided by Authority agent. This one will be able to investigate the content in clear (sensors data, buffered during abnormal disconnection of device, if it was any transmission trial to IoT platform handling sensors data).
6. Vendor representative notifies the Reputation System representative, through a signed / encrypted mail (optimally), about request to erase forever the Device ID in scope of investigation.
7. Vendor representative removes from Middleware all info belonging to Device ID in scope of investigation.
8. Vendor representative removes from Device the firmware.
9. Reputation system representative confirms (by phone calling / video-calling / physical meeting / other legal requested method) with Grid representative and IoT vendor representative, the request.
10. Reputation system representative erase forever the Device ID (and keep it in a “never use it again” list, to be checked for further changes). List is a local information, and it is up to Reputation if it wants to automate that for further definitions.

4.3 DOMAIN C – Medical IoT

4.3.1 Use case C1 – MIoT kit delivery – Patient registration and authentication

Validation scenarios overview

The C1 use case was validated using two scenarios: the first one, C1#1, targets a person/patient registration; and the second, C1#2, addresses the patient authentication in the MIoT services. In these scenarios two identification factors are employed – a hardware-based identification (based on SIM credentials) and a decentralized identification (based on SSI).

Validation scenario C1#1 description

This scenario depicts the process of a MIoT end user (person/patient) registering in the MIoT service. For this purpose, the medical IoT technology was integrated with the following ARCADIAN-IoT components and subcomponents: (1) Registration; (2) hardware-based identification and authentication (SIM-based); (3) Multifactor Authentication; and (4) the Self-Sovereign Identity (SSI). Additionally, components like Attestation, Reputation, Network-based Authorization and Behaviour monitoring were initialized for the newly created ARCADIAN-IoT ID.

Pre-conditions for the scenario:

- MIoT app is installed in an Android smartphone with a SIM provided by 1GLOBAL.
- The SIM needs to have 1GLOBAL security applets built in ARCADIAN-IoT and the MIoT app SHA1 signature in it (particularly in the ARA applet) for being authorized to use its functionalities. It also needs the SIM security applet middleware integrated with the MIoT app (within the Hardened Encryption component).
- The device needs to be configured to use an ARCADIAN-IoT private APN (private cellular network) for testing the network-based Authentication and Authorization components.
- The SSI Wallet App is downloaded & installed on mobile.
- The user opens the SSI IdP web page (frontend), inserts the requested identity data to be issued with a mobile wallet identity, and scans the QR Code from the mobile SSI Wallet and receives a natural person eID identity in their SSI Wallet.
  NOTE: This simulates the user having a mobile EU Digital identity Wallet issued with a national eID.
- The organization service is registered in the ARCADIAN-IoT Trusted Organization Registry with its Decentralized Identifier (DID:WEB) so that any person or device registrations to the ARCADIAN-IoT framework are validated by the associated DIDs signing key.
- The organization service provides a DID:WEB endpoint used for making its public signing key available.
- Reference Values sent to the Verifier to support smartphone attestation according to MIoT service policies.
- The Attester must be running on the smartphone.

The following actions are required for the validation:

1. The user opens the MIoT App and clicks on button to Register the patient.
2. User is asked to confirm its identity on the MIoT app and click to continue with the registration and create an identity in ARCADIAN-IoT framework. As part of this, the user is requested to present their Person Verifiable Credential from their mobile SSI Wallet and

upon successful verification an identity token is returned.
3. Next a registration request (signed by the DID associated to the registered trusted organization service) is sent to the ARCADIAN-IoT framework with the identity token and the mobile network token.
4. The ARCADIAN-IoT framework validates the registration request that is signed by a trusted organization service registered in the framework´s Trusted Organization Registry and creates a new aiotID if successful and is not previously registered.
5. User is informed on the MIoT app that their registration is complete.
6. A registration event is sent to the ARCADIAN-IoT Framework with their Person Identity and associated aiotID.
7. ARCADIAN-IoT Framework services (Reputation, Network-based Authentication and Authorisation, Device Behaviour Monitoring) initialise their respective services for the new aiotID.
8. Reputation System sends Attestation Cue triggering the attestation of the smartphone – the attestation is successful and contributes to the calculation of the initial reputation value.

Validation scenario C1#2 description

Following up to the registration, this scenario focuses on a person, particularly a patient, authenticating in MIoT services. This process, integrated within the whole MIoT solution, will allow to validate the following ARCADIAN-IoT components: (1) MFA; (2) hardware-based identification and authentication (SIM-based); and (4) the Self-Sovereign Identity (SSI). The expected result is to have a person authenticated using the two authentication factors.

The following actions were required for the validation:

1. Using the MIoT app the person will request to authenticate. The app attaches the ARCADIAN-IoT ID to the request (the one received upon registration).
2. Communicating through the cellular networks using 1GLOBAL SIM, when the request passes through the core network infrastructure, the ARCADIAN-IoT Notarizer appends to the authentication request a signed and protected Network ID token (transparent to the user).
3. The person authentication request reaches the MIoT backend services, which forwards the request to the MFA component.
4. The MFA splits the request received, asking: (1) the Network-based authentication component to confirm if the Network ID token issued by the core network (Notarizer) is valid and matches that ARCADIAN-IoT ID; (2) and the SSI component to validate the identity of that ARCADIAN-IoT ID.
5. The Network-based authentication components validate the received identifiers for that particular ARCADIAN-IoT ID and answer to the MFA with the result.
6. The SSI component establishes a secure communication with the SSI Wallet in the personal device to perform the verification of the person identity. The result is also sent to the MFA.
7. If the two authentication factors verification are positive (the two different identifiers correspond to the intended ARCADIAN-IoT ID) the MFA issues and signs a protected ARCADIAN-IoT ID Token and returns it to the MIoT backend, which returns it to the requesting personal device – the person/patient is now authenticated and can proceed with the use of the MIoT mobile app.
8. MFA also shares the results of the authentication events with other ARCADIAN-IoT components. This information is used by Behaviour monitoring to assess potential attacks and by the Reputation System to update the reputation of the involved entities - persons.

4.3.2 Use case C2 – MIoT capturing and sending vital signs and perceived health

status

Validation scenarios overview

The purpose of this scenario is to validate the process in which a patient's data is made available to their doctor and medical staff, ensuring the data is safely encrypted and made available only to those who are meant to access them.

The process involves data being sent from a monitoring device, through the SADP proxy, and through the Telemedicine web service.

Validation scenario C2#1 description

This use case refers to the health data sharing from the patient to the Telemedicine Web service, for making them available to the Doctor and her staff, as well as to other relevant services running in the Telemedicine Web Service e.g., alarm triggering as described in Section 3.4.2 (Use case C3) of D5.4.

Within the purpose of P1 validation, the following ARCADIAN-IoT components have been deployed and tested: Hardened Encryption, Self-Aware Data Privacy (SADP) and Remote Attestation. In P2, the integration with the Reputation System was added and validated.

The UML diagram relative to C2 in D5.3 illustrates the validation scenario described in the following paragraphs.

The following pre-conditions need to be validated due to the dependency that other use cases have on them:

a. The devices successfully receive the patient vital signs.
b. The device has the Hardened encryption library installed and can successfully connect to the SADP, which acts as a proxy service.
c. Proxy service receives device ID through JWT token, and verifies its signature to ensure validity
d. Proxy service uses attribute/public key to decrypt data.
e. Proxy service receives policies from the Telemedicine Web service.
f. Proxy encrypts data with received policies
g. Proxy informs Reputation System about the received request (RabbitMQ message)
h. The Telemedicine Service received encrypted data and stores it.
i. Telemedicine Web Service, Self-Aware Data Privacy, Hardened Encryption Libraries are deployed in the same secured environment e.g., physical machine.

The following actions are required for validating the use case:

1. The device collects patient vital signs captured by the medical sensors.
2. The MIoT app, which is authorized to communicate with the SIM (the SIM has its SHA1 signature for authorization), requests a new key pair generation in the SIM, through the Hardened Encryption library. These keys are going to be used for a Root of Trust (SIM) digitally signature flow. Upon request of the key pair generation the SIM returns the public key to the requesting Hardened Encryption method.
3. The device encrypts the data using Hardened Encryption library with a policy that the Self-Aware Data Privacy can access the data. It sends the encrypted data to the telemedicine web service.
4. The HTTP request containing the data is received by the SADP component.
5. The SADP component is provided with a valid key to verify token signature.
6. The security token received by the SADP component contains a valid signature.
7. The SADP component retrieves the encryption polices from the Telemedicine Web Service.

8. The SADP component leverages sends and encryption request to the HE library with the retrieved policies.
9. The HE library encrypts the data according to the retrieved policies and returns them to the SADP.
10. The SADP component sends the encrypted data to the telemedicine web service for their secure storage in the telemedicine database.
11. The SADP sends a message to the Reputation System containing the details of the request, allowing for reputation changes to be computed afterwards.

The Remote Attestation procedure is initiated via a manual trigger at the Verifier (running at a remote server); the attester (running in the smartphone) receives the associated attestation request (challenge) sent by the Verifier, collects the requested claims (dummy data at this stage), processes them (i.e., encapsulates them as Evidence) and sends the response to the Verifier. The Verifier displays the received Evidence, which should correspond to the claims displayed at the smartphone side.

4.3.3 Use case C3 – Personal data processing towards alarm triggering

Validation scenario overview

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.

Validation scenario C3#1 description

While Self-aware data privacy, Hardened Encryption (HE) and Reputation system components are used in this use case.

The starting point of the Use case is when new encrypted data originating from a patient's device (Use case C2) enters a database of the MIoT platform. The following actions are considered for validation:

1. A data processing Alert component (which is a part of the MIoT platform) requests encrypted data from the database.
2. When the data is obtained, the Alert component uses the HE component – that is, the HE encryption/decryption library -- to decrypt the parts of the encrypted data that are needed for the data processing. The assumption here is that the Self-aware data privacy component in C2 enforced the encryption with a policy that keeps the identity of the patient private, i.e., not exposed to the Alert component.
3. The result of the data processing, i.e., the alert, is encrypted (in such a way that only SADP component can access it) and forwarded to the SADP component, which decrypts it and further encrypts it (using the integrated HE encryption library) with an appropriate access policy.

The resulting encrypted alert is then saved at the MIoT platform database.

4.3.4 Use case C4 – Monitor a patient and update a patient monitoring protocol

Validation scenarios overview

The scenario considers a secure patient monitoring via medical IoT. Medical Professionals authenticate with multi-factor authentication, access encrypted patient data, edit it securely, and send commands to patient IoT devices, ensuring efficient communication and protocol adjustments while maintaining security.

Validation scenario C4#1 description

Scenario: The scenario involves secure patient monitoring by Medical Professionals authenticate with multi-factor authentication, access encrypted patient data, and send commands to patient IoT devices.

Prerequisite conditions:

a. Patient is previously registered in the MIoT mobile app as per Use case C1.
b. Medical Professional downloaded and installed SSI Wallet App on mobile.
c. Medical Professional is issued with a Person eID and an Organization Member Verifiable Credential to their SSI Wallet simulating the EU DIW.
d. Medical Professional is registered in the MIoT Hospital platform which is integrated with the ARCADIAN-IoT framework.
e. The Service Provider MIoT service is registered in the ARCADIAN-IoT Trusted Organization Registry with their Decentralized Identifier (DID:WEB) so that Organization Member registrations to the ARCADIAN-IoT framework are validated by the associated DIDs signing key and that the organization service is registered in the framework.

The following actions are required for the validation:

1. A medical professional accesses the MIoT hospital platform and chooses to be authenticated by **ARCADIAN-IoT multi-factor authentication** (based on previously registered mobile network authentication of the SIM and SSI Organization Member Verifiable Credential)
2. The medical professional is requested to open the mobile wallet before confirming to proceed so to be ready to receive a request on the mobile wallet for their Organization Member **Verifiable Credential**.
3. The medical professional confirms to present the Organisation Verifiable Credential on their wallet and sees that they are successfully authenticated in the MIoT hospital platform.
4. The medical professional is authorised by the **MFA ID Token** to accesses his/her patients´ dashboard to view any alerts or a specific patient´s data, upon verification of its signature and the user claims in the ID Token.
    a. As part of this authorization process the reputation of the medical professional is checked, and a low reputation would be a reason to deny access.
5. Medical professional login should be captured in MIoT hospital platform or SIEM.
6. The data that it receives comes from Use Cases C2 and C3 in encrypted form where the data was previously encrypted with **Hardened encryption**. The data is decrypted by the cryptographic keys that the medical professional is authorized to provision in the **Self-aware data privacy** module, and encrypted again with the correct policies that permit access to the data only to the authorized medical professionals.
7. The medical professional views patient data retrieved in real-time.
8. The patient is able to later revoke access to their data by a specific medical professional, and the health professional will subsequently not be able to view that patient´s data.

4.3.5 Use case C4 – Patient MIoT devices security or privacy incident

Validation scenarios overview

The following scenarios involve ensuring the validity of the data sent from the mobile devices to the telemed services. This involves ensuring the data wasn't tampered with by verifying the signature of the security tokens and informing the user to reset their devices and credentials in the event of a hack, or due to a malfunction in the devices.

Validation scenario C5#1 description

Name: Security token tampering

Scenario: This scenario is where the JWT security token sent alongside the data from a mobile device was tampered with, in order to send malicious data associated with a given device.

Mitigation: When a token is received by the SADP proxy, its signature is verified for validity. In the event the signature fails to verify the data is not sent to the Telemed service, and the information about the invalid token is logged.

Prerequisite conditions:

a. A key is provided to the SADP proxy to be used to verify token signatures (ES256 algorithm) via configuration (env variables)
b. Token signature verification is enabled

The following actions are required for the validation:

1. Data is sent to the proxy with a token carrying the wrong signature.
2. The proxy verifies the signature, and finds it invalid.
3. The data is not sent to the telemed service, and instead the proxy returns an error code response to the sender.
4. The failed verification is logged by the proxy service (optionally the reputation system is also informed) (RabbitMQ queue).
5. The CTI[7] component receives the alert. It converts the alert into MISP format and enriches it by adding threat level and class details to provide a better understanding of the potential threat. It then displays a warning message to alert the system operators or security analysts about the potential issue. Additionally, it sends an Indicator of Compromise (IoC) to the framework buffer to ensure that appropriate actions can be taken to mitigate the threat.
6. The Reputation System receives the alert information and updates the reputation of the device with the privacy incident. The update of the reputation score is also shared on the reputation updates exchange.

Validation scenario C5#2

Name: Credential and Self-Recovery

Scenario: This scenario is where the mobile device was hacked and all data on the mobile was corrupted or lost and is then recovered.

Mitigation: The user is recommended to perform a factory reset and re-install the SSI Wallet and recover their previously issued credentials.

Prerequisite conditions:

a. The wallet app must be previously issued with a Person Verifiable Credential (VC)
b. The user is registered in the patient app

The following actions are required for the validation:

1. The VC is backed up in the wallet app.
2. The user enters in settings mode and deletes all the wallet app.
3. The user selects the mobile wallet app again and is asked to provide fingerprint registration and gains access to the wallet app.
4. The user then proceeds to restore the wallet credentials.
5. The user selects recovery in the patient app which instructs the user to create a new wallet

[7] The CTI system is pre-loaded with ML models. While their evaluation was done in WP3, the training of the event classification module, which includes features from the Federated AI component, underwent separate validation for demonstration purposes. A description of this validation involving three distributed entities is provided in Appendix D.

connection as part of the recovery, for the users registered email. This can be requested on the SSI IdP frontend or alternatively on the patient app.
This must be accepted on the mobile wallet app.

6. The user continues the recovery process on the patient app, which performs a re-registration. If the identity has been previously registered a 409 conflict error code will be returned with the associated aiotID.
7. The user requests the patient app authentication for the aiotID and is successfully logged in after the user: 1. presents the VC from the wallet app, 2. Succeeds in the face authentication and 3. mobile network authentication is successful.
8. The user requests any backed up data in self-recovery to be restored also to the patient app.

4.3.6 Use case C6 – MIoT cloud services security or privacy incident

Validation scenarios overview

This specific use case focuses on the mitigation of a Distributed Denial of Service (DDoS) attack, orchestrated by a combination of infected IoT medical devices forming a controlled botnet and external devices originating from the internet. The attack targets the medical servers responsible for IoT medical devices hosted by RGB. In this case, authentication for User Equipment is conducted in according to standards with the 1GLOBAL SIM card. To validate the mitigation capabilities, legitimate devices are continually generating network traffic at a rate of 80-100 Mbps, while the malicious traffic attempts to saturate the network with up to 500 Mbps, which means disrupting network resources for legitimate users.

Validation scenario C6#1 description

Motivation

The primary motivation behind this validation scenario is to demonstrate the efficacy of the Cognitive Self-protection loop, comprised of the three core software components (NFM, NSH, and NSP). The goal is to showcase that this autonomous loop can effectively detect, plan, and mitigate incoming threats without the need for human intervention and within a reasonable timeframe.

The infection and attack launch

1. The MIoT devices are connected and authenticated to the network infrastructure.
2. The MIoT devices are authenticated in the health services of RGB.
3. The MIoT devices start sending health metrics and data to the medical services.
4. Part of the MIoT devices is infected and added to the botnet.
5. The MIoT devices and other outsider devices launch a coordinated DDoS attack against the medical services allocated in the RGB premises.

The Cognitive Self-protection Loop

1. The traffic flowing through the network infrastructure is being mirrored to a Management Layer.
2. The network topology is being monitored and published by the Resource Inventory Agent (RIA) – a subcomponent of the Network Self-healing (NSH) – periodically.
3. The Network Flow Monitoring (NFM), located in the Management Layer, is sensing, and analysing the mirrored network flows.
4. Multiple flows match with the NFM detection rules, and this component builds the necessary alert with the full network flow information.
5. The NFM raises a Network IDS Event to the message bus exchange.
6. The NSH consumes the Network IDS Event from the message bus queue.
7. The NSH checks the very current network topology information.

8. The NSH produces a set of prescriptive analytics to build the necessary Healing Actions to mitigate the threat.
9. The NSH obtains the *What* to do, *When* to do, *Where* to do and *For How Long* to do actions.
10. The NSH sends a set of intent-based Healing Actions to the message bus exchange.
11. The Network Self-protection (NSP) consumes the Healing Actions from the message bus queue.
12. The NSP creates a Protection Rule OpenFlow-based and enforces it in the data plane in the exact topology interface that the NSH specified in the Healing Actions.
13. The NSP checks that the Protection Rule has been added successfully in the data plane and sends a confirmation to the Network Self-protection Confirmation message bus exchange.
14. The NFM consumes the confirmation from the NSP that the malicious flow has been dropped successfully and tags the flow as DROPPED.

4.3.7 Use case C7 – Medical 3rd party security or privacy incident

Validation scenarios overview

The following scenario involves ensuring the integrity of the data transmitted from the telemed services to staff member tablets. This includes verifying that the data has not been altered by confirming the security token signatures and instructing the user to reset their devices and credentials in case of a breach or device malfunction.

Validation scenario C7#1 description

1. Validation Preparation:
    a. Ensure that all partner components (UWS, RGB, UC, RISE, 1GLOBAL and IPN) are operational and integrated within the ARCADIAN framework.
    b. RGB has provided the final versions of their services/apps for Domain C, which includes the web app for medical staff to connect to the cloud service where patient data is kept.
2. Integration Check:
    a. Verify that UWS NFM and NSP are correctly sending NFM Events and Healing Instructions to the IPN RabbitMQ message broker.
    b. Ensure that CTI (RISE) and RS (UC) are set up to consume the NFM events messages from the IPN RabbitMQ.
    c. Confirm that the RGB IoT-device Traffic emulator is functional and can emulate multiple users sending traffic to the cloud service.
3. Validation Execution:
    a. Launch a simulated DDoS attack, targeting the cloud service to validate the resilience and healing instructions within the ARCADIAN framework.
    b. Confirm that the UWS loop (NFM-NSH-NSP) detects and mitigates the attack successfully for all considered scenarios, including C7.
    c. Re-run the testbed with the necessary minor modifications to target not only the cloud service (C6) but also the medical web app (C7).
    d. Validate that the system can differentiate between the targets and that the IDS events are automatically sent to the CTI during the attack scenarios.
    e. Ensure that CTI (RISE) and RS (UC) respond accordingly to the events triggered by the attack.

5. ARCADIAN-IOT FRAMEWORK EVALUATION

The complete list of KPIs associated to each ARCADIAN-IoT component was identified during WP3 and WP4 execution. Some of the KPIs were addressed in the context of WP3 and WP4 (or even WP6, e.g., in case of training-related KPIs). A relevant subset of the KPIs were also scoped for verification in the scope of use case validation activities, (T5.5), based on the prototyping activities (first P1, and now P2). The latter subset of KPIs is summarized below and organized according to the associated Vertical or Horizontal plan. Further analysis of the KPIs value achievements as a result of P2 validation activities are then provided.

5.1 Vertical Components KPIs

This section provides the analysis over Vertical Component KPIs (established in D4.3 [8]) which are relevant within use case validation scope, the associated measurable indicators, target and achieved values. Table 2 summarizes the KPI scope (or features) and the associated validation scenario(s), while the remaining details are presented throughout the rest of the section.

Table 2 - Evaluation KPIs associated to components from the Vertical planes

Plane	Component	KPI scope	Supporting Validation scenario(s)
Identity	Decentralized Identifiers	Support availability of decentralized identity management schemes	A2#1, C1#1
		Support authentication for persons and IoT devices	A2#1, A4#1, C1#1
	Network-based authentication of IoT devices in third-party services	Leverage cellular network authentication processes in a new zero-touch authentication of IoT devices in third-party services	A1#1, A2#1, A5#1, C1#1
	Biometrics	Low inference time for Face Verification Algorithm	A2#1, A5#1
		Low End-to-End delay of the biometric process	A1#1, A2#1, A5#1
		High accuracy of the Face Verification Alg. (<2m)	A2#1
		High accuracy of the Face Verification Alg. (>2m)	A5#1
		Reliable recognition of the face (<2m)	A2#1
		Reliable recognition of the face (>2m)	A5#1
		Cost-effective camera and drone platform	NA
	Multifactor Authentication	Multifactor authentication component joining hardware-based identification, decentralized identification and biometrics (for the case of persons)	A2#1, A5#1
Trust	Verifiable Credentials	Support interop with one eIDAS	A1#1,

		schema	A2#1, C1#1
	Network-based Authorization	Enforcement of the defined model for trust, security, and privacy, being an autonomous agent able of receiving inputs from ARCADIAN-IoT Reputation System to enforce security actions	A6#1
		Self and coordinated healing with reduced human intervention, by informing the SIM of device's trustworthiness information, triggering the subsequent SIM-based protection and recovery actions	A6#1
	Reputation System	Number of messages analysed per unit time	NA
		Time required to determine reputation	NA
		Type of entities supported	Most validation scenarios
		Computational resources consumption	NA
	Remote Attestation	Novel RATS-based Remote Attestation procedure	A6#1, B4#1, C5#1
		Attestation Results feeding both device and service reputation models	A6#1
Recovery	Self-Recovery	Backups with hardened encryption, supporting decryption policies	A6#1, A7#1, C5#2
		Working in conjunction with modern networked filesystems focusing on scalability and performance for remote backup storage	A7#1
		Multiplatform client-side support	A6#1, A7#1
	Credentials Recovery	Support Credential Recovery operations after security/privacy incidents for persons and IoT Devices	A6#1, C5#1
		Availability of self-recovery and decentralized identity management schemes	A6#1, C5#1

5.1.1 Decentralized Identifiers KPIs

The KPIs for the DID component are reported in Table 3.

Table 3 - KPI Summary for Decentralized Identifiers

Feature/Scope	Metrics	Target values	Achieved value
Support availability of decentralized identity management schemes	Support at least two of the use case domains	>=2	3
Support authentication for persons and IoT devices	Support “Persons· & “IoT Devices”	3	5 Persons, Constrained IoT Devices, Services, Organization Members & IoT Devices

5.1.2 Network-based authentication KPIs

The KPIs for the Network-based Authentication component are reported in Table 4.

Table 4 - KPI Summary for Network-based Authentication

Feature/Scope	Metrics	Target values	Achieved value
Leverage cellular network authentication processes in a new zero-touch authentication of IoT devices in third-party services	Number of different devices where the innovation is demonstrated	>=2	2 device types (IoT and personal) communicating with 2 protocols (HTTP and MQTT)
	TRL	>=6	6

5.1.3 Biometrics KPIs

The KPIs for the Biometrics component are reported in Table 5.

Table 5 - KPI Summary for Biometrics

Feature/Scope	Metrics	Target values	Achieved value

Low Inference Time for Face Verification Algorithm	Frames per Second (FPS) or Milliseconds (ms)	16 FPS / 62.5 ms	18 FPS/ 55.56 ms
End-to-End speed of the biometrics process	Frames per Second (FPS) or Milliseconds (ms)	5 FPS / 200 ms	7 FPS / 142.9 ms
High accuracy of the face verification algorithm at close distances (less than 2 meters).	mean Average Precision (mAP)	Over 90% mAP	90.99% mAP
Reliable Recognition of the Face Verification Algorithm at close distances (less than 2 meters).	False Acceptance Rate (FAR)	Below 0.5% FAR	0.49 % FAR
High accuracy of the face verification algorithm at far distances (more than 2 meters).	mean Average Precision (mAP)	Over 70% mAP	71.81% mAP
Reliable Recognition of the Face Verification Algorithm at far distances (more than 2 meters).	False Acceptance Rate (FAR)	Below 0.5% FAR	0.46 % FAR
Cost-effective camera and drone platform (hardware only).	Euros (€)	500€	500€

Biometrics KPIs were evaluated in WP4 and reported in the Deliverable 4.3.

5.1.4 Multi-factor Authentication KPIs

The KPIs for the MFA component are reported in Table 6.

Table 6 - KPI Summary for Multi-factor Authentication

Feature/Scope	Metrics	Target values	Achieved value
Multifactor authentication component joining hardware-based identification, decentralized identification and biometrics (for the case of persons	Number of simultaneous different identification factors for persons	3	3
	Number of simultaneous different identification factors for devices	2	2
	Number of devices used simultaneously in a person's identification	2	2

5.1.5 Verifiable Credentials KPIs

The KPIs for the VCs component are reported in Table 7.

Table 7 - KPI Summary for Verifiable Credentials

Feature/Scope	Metrics	Target values	Achieved value
Support interop with one eIDAS schema	Issue person Verifiable credential with an eIDAS compatible schema	Person schema to be supported as per EBSI schema: https://ec.europa.eu/digital-building-blocks/code/projects/EBSI/repos/json-schema/browse/schemas/ebsi-vid/natural-person/2022-11/schema.json	Person schema is supported as per EBSI schema that follows eIDAS.

5.1.6 Network-based Authorization KPIs

The KPIs for the Network-based Authorization component are reported in Table 8.

Table 8 - KPI Summary for Network-based Authorization

Feature/Scope	Metrics	Target values	Achieved value
Enforcement of the defined model for trust, security, and privacy, being an autonomous agent able of receiving inputs from ARCADIAN-IoT Reputation System to enforce security actions	Automatic bidirectional communication authorization enforcement for devices and people according to trustworthiness levels and its dynamic changes related with security events (Y/N)	Achieved	Achieved
	Time to enforce the authorization policy after the network being informed	Near real time	<1second
Self and coordinated healing with reduced human intervention, by informing the SIM of device's trustworthiness information, triggering the subsequent SIM-based protection and recovery actions	Ability to securely inform the eSIM of devices trustworthiness level (Y/N)	Achieved	Achieved
	Use of eSIM in device self-protection and self-recovery actions (Y/N)	Achieved	Achieved
	Number of different devices where the innovation is demonstrated	>=2	Achieved (all cellular devices used in the IoT domain use

			cases where reputation is able to infer trustworthiness)

5.1.7 Reputation System KPIs

The KPIs for the Reputation component are reported in Table 9.

Table 9 - KPI Summary for Reputation System

Feature/Scope	Metrics	Target values	Achieved value
Number of messages analysed per unit time	Messages per second (s)	100 msg / s	100 msg / s
Time required to determine reputation	Elapsed time to determine reputation (s)	<= 1 s	100 ms
Type of entities supported	Number of different entities that are supported	3	3
Computational resources consumption	%of CPU, % of Memory, % of storage, I/O Bytes	< 25 % < 25% < 25 %	5% 0.1% 5%

5.1.8 Remote Attestation KPIs

The KPIs for the Remote Attestation component are reported in Table 10.

Table 10 - KPI Summary for Remote Attestation

Feature/Scope	Metrics	Target values	Achieved value
Novel RATS-based Remote Attestation procedure	*Number of devices/OS platforms supported by remote attestation*	2	2
Attestation Results feeding both device and service reputation models	Types of IoT devices reputation affected by RA	1	2

	Number of IoT services reputation affected by RA	1	1

Regarding the *"Number of devices/OS platforms supported by remote attestation*", RA has been integrated and validated in smartphones in diverse use cases, including regular usage (A1, A2, A3, C1, C2, C5) and attack to the attestation process (A7). RA has also been successfully validated in the drone's Linux environment (Ubuntu OS) in two use cases: A4 and A6.
With respect to the usage of attestation results for feeding device and service reputation models, Both KPIs depend on the following features:

- The ability for the Verifier to generate Attestation Results based on received Evidence à validated
- The ability for the Reputation System to process / appraise Attestation Results, which may lead to updates in the Reputation of a Device à validated

More concretely, the KPI on "*Types of IoT devices reputation affected by RA*" has been validated for affecting smartphones reputation in use cases A1, A2, A3, C1, C2, C5, and for affecting drones' reputation in A4 and A6. As for KPI "*Number of IoT services reputation affected by RA*" it has been validated for affecting DGA service in all use cases where the drone was attested (A4, A6).

5.1.9 Self-Recovery KPIs

The KPIs for the Self-Recovery component are reported in Table 11.

Table 11 - KPI Summary for Self-Recovery

Feature/Scope	Metrics	Target values	Achieved value
Backups with hardened encryption, supporting decryption policies	Different access permissions allow decryption of different data backup types (logs, configuration files, generated or stored data; integration with HE)	Achieved	Achieved
Working in conjunction with modern networked filesystems focusing on scalability and performance for remote backup storage	Ability to scale storage capabilities according to current requirements.	Achieved	Achieved
Multiplatform client-side support	Demonstrate backup/recovery on at least 2 devices	2 devices	2 devices

5.1.10 Credentials Recovery KPIs

The KPIs for the Credentials Recovery component are reported in Table 12.

Table 12 - KPI Summary for Credentials Recovery

Feature/Scope	Metrics	Target values	Achieved value
Support Credential Recovery operations after security/privacy incidents for persons and IoT Devices	Credential Recovery mechanisms supported.	1	2
Availability of self-recovery and decentralized identity management schemes.	Support recovery of Decentralized Identifiers and Verifiable Credentials.	Recovery supported	Recovery supported

5.2 Horizontal Components KPIs

This section provides the analysis over Horizontal Component KPIs (established in D3.3 [7]) which are linked to the validated use cases, the associated measurable indicators, target and achieved values. Table 13 summarizes the KPI scope (or features) and the associated validation scenario(s), while the remaining details are presented throughout the rest of the section.

The covered KPIs have been validated through

Table 13. Evaluation KPIs associated to components from the Horizontal planes

Plane	Component	KPI scope	Supporting Validation scenario(s)
Privacy	Self-aware Data Privacy	Making sure the protection algorithm is flexible and can adapt to different needs	B1#1, C2#1
		Making sure the component is usable and can simplify the issuing of policies by the users.	B1#1, C2#1, C3#1, C4#1
Security	Cyber Threat Intelligence	Enable the aggregation and processing of IoCs generated by internal or external sources	A6#1, A7#1, C5#1, C6#1, C7#1
	Device Behaviour Monitoring	Ability to process different input types with non-root privileges (syscalls, auth, rep)	A6#1, B4#1
		Deployment in heterogenous devices	A1#1, B1#1, C#1
	Network Flow Monitoring	Provide new alert metadata information about IoT and 5G flow structure, within the supported network segments with a number of >= 4 (Edge, Core, RAN and Transport).	C6#1, C7#1

		Provide transversal detection capabilities to protect, simultaneously tenant infrastructure and the infrastructure provider by supporting >=4 encapsulations and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures such as VXLAN, GRE, GENEVE and GTP.	C6#1, C7#1
	Network Self-Healing	Provide self-healing for overlay networks and IoT networks supporting >= 4 encapsulation and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures such as VXLAN, GRE, GENEVE or GTP.	C6#1, C7#1
		Provide dynamic and distributed enforcing of protection/healing policies in 7 or more network segments (Edge, Core, RAN, Transport, Backbone, Enterprise, Backhaul, Midhaul).	C6#1, C7#1
		Provide network topology understanding to reduce human intervention (towards 0% of human intervention) supporting the coordination of recovery to pre-defined trust levels (>= 95% of flow services before anomalous behaviour) using such topology.	C6#1, C7#1
	Network Self-Protection	Novel traffic classifier able to deal with data paths in 4G/5G IoT networks (overlay traffic with several levels of nested encapsulation)	C6#1, C7#1
		OpenFlow protocol extension to provide a flexible and extended programmability of the data plane.	C6#1, C7#1
		% Human intervention strictly required, in healing and recovery procedures.	C6#1, C7#1
		OVS Netlink API extension for inter-process communication kernel-user space	C6#1, C7#1
	IoT device self-protection	Policy enforcement based on ensemble of risk levels, indicators of compromise, reputation and threat information.	A6#1
		Autonomous self-protection mechanism for heterogeneous operating systems and devices.	A6#1, C5#1
Common	Hardened Encryption (with SIM)	Encryption library with fine access control	A1#1, C1#1
		Number of types of platforms/devices demonstrated	A1#1, C1#1
		Efficient implementation of encryption/decryption	A1#1, A2#1, A3#1, A4#1, C2#1, C3#1, C4#1

	Hardened Encryption (with cryptochip)	Simplified IoT middleware and device provisioning/fulfilment	B1#1
		Encryption speed up with multiple segments (TLS, Hardened Encryption)	B2#1
	Permissioned blockchain	Using the permissioned blockchain to publish trusted information to third parties in the ARCADIAN-IoT framework.	A6#1, A7#1
		Deployment of permissioned blockchain in IoT environment.	A2#1

5.2.1 Self-aware Data Privacy KPIs

The KPIs for the SADP component are reported in Table 14.

Table 14 - KPI Summary for Self-Aware Data Privacy

Feature/Scope	Metrics	Target values	Achieved value
Making sure the protection algorithm is flexible and can adapt to different needs	Number of potential policies handled by the protection algorithm	5	>5
Making sure the component is usable and can simplify the issuing of policies by the users.	Usability of the policing issuer (Likert scale).	90%	80%

The number of policies supported include direct integration of the Hardened Encryption library, an anonymisation technique implemented directly, and 10+ encryption policies supported via a library integrated into the SADP proxy service.

The UI that was developed to interact with the creation of policies in the SADP component was in general well accepted, however the feedback we gained from internal testing suggested there is still room for improvement in several areas e.g. navigation flow and button intuitively. For this reason, we were not able to achieve the target value but a very close one and, in any case, a very positive score.

5.2.2 Federated AI KPIs

The KPIs of the Federated AI Component were not assessed in this specific deliverable. All KPIs associated with this component, were covered in Deliverable D3.3 [7].

5.2.3 Cyber Threat Intelligence KPIs

The KPIs for the CTI component are reported in Table 15.

Table 15 - KPI Summary for Cyber Threat Intelligence

Feature/Scope	Metrics	Target values	Achieved value
Enable the aggregation and processing of IoCs generated by internal or external sources	Number of the types of threat managed	5	13
	Number of different IoC formats supported	3	5

The evaluation shown above was done via the integration of this component with Domain A use cases with active engagement in A6 (drone security or privacy incidents. Similarly, in Domain C this component had an active engagement on use case C5, C6 and C7 (security or privacy incident). The evaluation is considered successful as it has achieved the target values initially proposed.

Regarding the KPI "Number of types of threats managed," the CTI component has been confirmed to handle 13 types of threats, including APT, Attack, Backdoor, Botnet, Command and Control, Exploitation, Malspam/Phishing, Malware, Misinformation, Ransomware, Trojan, and Alerts sent by the DBM component. As for the KPI "Number of different IoC formats supported," the CTI component has been tested with 5 different IoC formats, including device alerts generated by DBM, the flow alert generated by NFM, the token validation message crafted by SADP, the original STIX format, and the MISP format.

5.2.4 Device Behaviour Monitoring KPIs

The KPIs for the DBM component are reported in Table 16.

Table 16 - KPI Summary for Device Behaviour Monitoring

Feature/Scope	Metrics	Target values	Achieved value
Ability to process different input types with non-root privileges (syscalls, auth, rep)	Number of inputs considered	3	3
Deployment in heterogenous devices	Number of supported devices	2	2

The evaluation shown above was done via the integration of this component with all Domain A use cases (A1 to A7), Domain B uses cases B1, B2 and B4, as well as Domain C use cases C1 to C5. The evaluation is considered successful as it has achieved the target values initially proposed.

With respect to the number of inputs considered, as it was mentioned before, we have verified that the Device Behaviour Monitoring (DBM) component was successfully deployed on the Drone Hardware from Domain A and on the IoT gateway (i.e., smartphone) interfacing the Medical IoT device in Domain C. The DBM was also deployed alongside the DGA app (Android) on Domain A. In addition, it was possible to verify that the DBM can be effectively deployed within a microservice (in a container) to monitor the system calls of the service and detect anomalous behaviours within the service - this extra capability (a nice to have feature) was verified within the scope of Domain B integration activities but was ultimately not put into place due to the need of changing the deployment approach of Domain B Middleware.

The ability of processing different input types was also successfully evaluated. System calls are being processed in the drone deployment; authentication events are being processed in all use case deployments; and reputation information is also being processed in all use case deployments.

5.2.5 Network Flow Monitoring KPIs

The KPIs for the NFM component are reported in Table 17.

Table 17 - KPI Summary for Network Flow Monitoring

Feature/Scope	Metrics	Target values	Achieved value
Provide new alert metadata information about IoT and 5G flow structure, within the supported network segments with a number of >= 4 (Edge, Core, RAN and Transport).	Number of network segments supported to get the metadata information.	>= 4	= 4
Provide transversal detection capabilities to protect, simultaneously tenant infrastructure and the infrastructure provider by supporting >=4 encapsulations and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures such as VXLAN, GRE, GENEVE and GTP.	The number of supported encapsulations and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures.	>=4	=4

The network segments supported by the NFM to get the metadata information about the malicious flow detected are the Edge, Core, RAN and Transport. Additionally, the supported encapsulations tested and achieved as tunnelling protocols are GTP, GRE, GENEVE and VXLAN. These KPIs are validated in the use case C6, where a 4G/5G-IoT network topology is used as the scenario of the use case. As well as the attack launch over the full infrastructure with the multiple flow morphologies along the entire network, thus providing the results of the network segments and network encapsulations supported in the detection of the attacks.

5.2.6 Network Self-Healing KPIs

The KPIs for the NSH component are reported in Table 19.

Table 18 - KPI Summary for Network Self-Healing

Feature/Scope	Metrics	Target values	Achieved value
Provide self-healing for overlay networks and IoT networks supporting >= 4 encapsulation and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures such as VXLAN, GRE, GENEVE or GTP.	The number of supported encapsulations and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures.	>= 4	=4
Provide dynamic and distributed enforcing of protection/healing policies in 7 or more network segments (Edge, Core, RAN, Transport, Backbone, Enterprise, Backhaul, Midhaul).	Number of network segments supported to get the metadata information.	>= 7	=7
Provide network topology understanding to reduce human intervention (towards 0% of human intervention) supporting the coordination of recovery to pre-defined trust levels (>= 95% of flow services before anomalous behaviour) using such topology.	% Recovery of the flow services prior to anomalous behaviour.	>95%	=97.5%
	Reduce human intervention to the strictly required, in healing and recovery procedures.	Towards 0%	Towards 0%

The network segments supported by the NSH to get the metadata information about the network topology detected are the Edge, Core, RAN, Transport, Backbone, Enterprise, Backhaul and Midhaul. Additionally, the supported encapsulations tested and achieved as tunnelling protocols are GTP, GRE, GENEVE and VXLAN. These KPIs are validated in the use case C6, where a 4G/5G-IoT network topology is used as the scenario of the use case. Additionally, the attack covers the entire infrastructure, leveraging multiple topology morphologies across the network, thereby generating results on network segments and supported network encapsulations for attack detection. In the described use case, the NSH achieves close to 100% service recovery, restoring normal behaviour post-attack. Given the automation of the security cognitive loop, there is no human intervention required throughout the phases of detection, planning, and mitigation of the attack.

5.2.7 Network Self-Protection KPIs

The KPIs for the NSP component are reported in Table 19.

Table 19 - KPI Summary for Network Self-Protection

Feature/Scope	Metrics	Target values	Achieved value
Novel traffic classifier able to deal with data paths in 4G/5G IoT networks (overlay traffic with several levels of nested encapsulation)	Support encapsulation and tunnelling protocols widely used in overlay networks inherent to 4G/5G IoT mobile infrastructures such as VXLAN, GRE, GENEVE or GTP, for instance.	>= 4	= 4
OpenFlow protocol extension to provide a flexible and extended programmability of the data plane.	% Recovery of the flow services before anomalous behaviour.	>95%	= 100%
	Reduce human intervention to the strictly required, in healing and recovery procedures.	Towards 0%	= 0%
OVS Netlink API extension for inter-process communication kernel-user space	Number of different flows mitigated	Up to 10e6 malicious flows	= 2e20 malicious flows
	Bandwidth performance	Up to 10 Gbps	= 13.82 Gbps

5.2.8 IoT device self-protection KPIs

The KPIs for the DSP component are reported in Table 20.

Table 20 - KPI Summary for IoT Device Self-Protection

Feature/Scope	Metrics	Target values	Achieved value
Policy enforcement based on ensemble of risk levels, indicators of compromise, reputation and threat information.	Number of policy enforcement methods	3	3
Autonomous self-protection mechanism for heterogeneous operating systems and devices.	Type of supported operating systems and type of device	2	2

The evaluation shown above was done via the integration of this component with Domain A use cases with active engagement in A6 and A7 (security or privacy incidents) and a passive engagement on A1 to A5 use cases. Similarly, in Domain C this component had an active

engagement on use case C5 (security or privacy incident) and a passive engagement on C1 to C4.
With respect to the number policy enforcement methods, the Device Self Protection (DSP) supported policy enforcement based: 1) indicators of compromise (sent by the CTI component), 2) device reputation (provided by the reputation system), and 3) threat information (provided by the Device Behaviour Monitoring).
Regarding the type of supported operating systems and device types, the DSP allows the deployment on Linux and Android Operating Systems, which also translate into a possible deployment on the Drone and on the IoT Gateway (i.e., smartphone).

5.2.9 Hardened Encryption (with SIM)

The KPIs for the eSIM-based Hardened-Encryption component are reported in Table 21.

Table 21 - KPI Summary for Hardened Encryption (with SIM)

Feature/Scope	Metrics	Target values	Achieved value
Encryption library with fine access control	Number of API,	>= 4	5
	number of types of platforms/devices demonstrated	>= 2	3
Efficient implementation of encryption/decryption	Computation time	Comparable to state of the art on multiple devices	achieved
Add Root of Trust information to encrypted data with SIM-based signatures	Use of SIM as RoT in hardened encryption processes	Y	Y
	SIM time to sign a payload (SHA256)	< 2 seconds	~0.5 seconds
	Number of different devices where the innovation is demonstrated	2	2

Encryption library with fine access control: The HE library has been successfully integrated in an Android App using provided Java interface and has been tested on an Android 11 smart phone, as part of the Use Case C2. Moreover, the library with Python bindings has been integrated at the server side of the MIoT service, running on a Linux server, as part of C3. ARCADIAN IoT Self-aware data privacy component has integrated the Go based HE library in C2 and C3. Finally, also ARCADIAN IoT Attestation components has integrated the library with

Python APIs to secure attestation data (A1, A3, C2). We conclude that 3 APIs to the library have been validated and that the use of the library was demonstrated on (at least) two (chip architecture wise) different devices. As part of P2, additional API in JavaScript, that will be used on smartphones, servers and personal devices in a browser, will be validated to complete the KPI.
Efficient implementation of encryption/decryption: The approach to provide efficient implementation of the encryption and decryption processes is based on an optimized implantation of the protocols in Go which is then cross-compiled to shared objects that bindings to other (less efficient) programming languages can use. The reference value that we use is based on ABE implementation paper here the following values were reported: Encryption/Decryption on a laptop with 1.60GHz Intel Quad-Core i7 approx. 160ms/approx. 250ms for a policy with 5 attributes, Encryption/Decryption on an Android phone with 1.60GHz Intel x86 processor approx. 2.5s/approx. 6s for a policy with 5 attributes. We note that a different encryption scheme was used than in the mentioned paper but with comparable functionality. Moreover, the messages sent in the Use cases are longer. The evaluation of encryption was done on a Samsung Galaxy A10 Android phone with a 64bit 1.6GHz processor with ARM architecture running in 32bit mode. The encryption (as part of Use Case C2) takes approx. 720ms where the encryption policy has one attribute. The decryption was evaluated on a backend server (as part of Use Case C3) with a 4-core Intel i7 7th Gen processor, taking approx. 280ms to complete. We conclude that the values are comparable to the state-of-the-art values, and that the HE component can be applied to the setting of the Use Cases.
Add Root of Trust information to encrypted data with SIM-based signatures: With respect to the KPI on “number of devices where the innovation was demonstrated”, it is highlighted that the SIM security applet is agnostic to the device where it runs, if it has a SIM with the cryptographic capabilities needed (most of the current SIMs have). However, to communicate with the SIM, there is a need for a device middleware running at the device. Both an Android and Python middleware libraries were provided for demonstration in 2 distinct devices (according to IoT solution providers requests): smartphone and drone; for Android, an authorization SIM applet had to be delivered as well, where the apps entitled to communicate with the SIM are identified.

5.2.10 Hardened Encryption (with cryptochip)

The KPIs for the cryptochip-based Hardened Encryption component are reported in Table 22.

Table 22 - KPI Summary for Hardened Encryption (with crypto chip)

Feature/Scope	Metrics	Target values	Achieved value
Simplified IoT middleware and device provisioning/fulfilment	Provisioning time (for any scenario) into device side, with GUI in place and how to procedure, into device side.	<= 5 min	Between 2 and 5 minutes
	Provisioning time (for any scenario) with web dedicated page in place and how to procedure, into middleware side.	<= 2 min	Between 1 and 2 minutes

Encryption speed up with multiple segments (TLS, Hardened Encryption)	T1_E – Time duration between sensors data stream aggregation and encrypted payload generation, by device firmware agent designed and build for encryption. This indicator is applicable for sense device – to – IoT platform.	T1_E <= 2s	Between 1 and 2 seconds
	T4_D – Time duration between encrypted payload receiving and actuators “in clear” commands, by same device firmware agent. This indicator is applicable for sense IoT platform – to – device.	T4_D <= 6s	Between 2 and 6 seconds
	T3_E – Time duration between encrypted TLS payload received from IoT platform, decryption by certificate applied, and encryption with correspondent hardware key of the payload, by dedicated local middleware agent. This indicator is applicable for sense IoT platform – to – device.	T3_E <= 4s	Between 2 and 4 seconds
	T2_D – Time duration between receiving the encrypted payload received from device and decryption by correspondent hardware key of the payload, by dedicated local middleware agent, and relaying forward by TLS to IoT platform. This indicator is applicable for sense device – to – IoT platform.	T2_D <= 8s	Between 3 and 8 seconds

Provisioning time (for any scenario) into device side supposed building a Command Line Interface, and a debugging messages chapter using a PLC / SCADA operations logic, to simplify operator decisions and map all changes into a logical & hierarchical structure. These support tools were designed, deployed and used. They will remain as components of solution during commercial exploitation.

Provisioning time (for any scenario) into Middleware side supposed building a front end for this purpose, which was successfully realized using UX best practices and IoT specific knowledge base.
Operation speed depends by user training, but once this is done, user can move fast & precise into CLI of device and Middleware front end.
Regarding **encryption and decryption time KPI's**, we have observed these are hardly influenced indirectly by type of communication network technology chosen (GSM, LTE, ETH, etc.). Anyhow, after many trials with device in fixed location or on move (at high speed, in train, exposed to many disconnections, handovers or traffic data bear congestion), we have validated a robust encryption and decryption mechanism, without any authentication or traffic sessions aborted / interrupted. We have also validated that encryption and decryption system will not tolerate any network error or process missing information, just to validate the device connectivity to Middleware or traffic sent by this one to Middleware. KPI's time refining were performed mainly by firmware optimization (edge computing agent for sensors data management, manipulation of the other firmware agents – for encryption, for communication).

5.2.11 Permissioned blockchain KPIs

The KPIs for the Permissioned blockchain component are reported in Table 23.

Table 23 - KPI Summary for Blockchain

Feature/Scope	Metrics	Target values	Achieved value
Using the permissioned blockchain to publish trusted information to third parties in the ARCADIAN-IoT framework.	Number of ARCADIAN-IoT services using permissioned blockchain	3	3
Deployment of permissioned blockchain in IoT environment.	Number of peer nodes deployed	3	3

5.3 Achievement of Project Objectives

The Project Objectives were enumerated in the previous P1 D5.4 deliverable (section 7) and included the achievements at that time for the complete 7 Objectives and their correspondent KPIs. The list is summarized in Table 24:

Table 24 - Project Objectives and related KPIs summary

Objectives	Key Performance Indicators (KPIs)
Objective #1 To create a decentralized framework for	Objective verified through the existence and readiness of the framework. No specific KPIs assigned to this objective.

IoT systems - ARCADIAN-IoT framework				
Objective #2 Enable security and trust in the management of objects' identification	KPI2.1 Support, at least, two identity approaches at hardware level (SIM and CryptoChips)	KPI2.2 Avoid single trusted entities through decentralized approaches (SIM identity approach)	KPI2.3 Support, at least two robust identity mechanisms for devices and apps/services	
Validation scenarios supporting KPI validation	SIM: validation scenarios from domains A and C Cryptochips: validation scenarios from domain B	A2#1, C1#1	C1#1	
Objective #3 Enable distributed security and trust in management of persons' identification	KPI3.1 High accuracy in facial recognition AI models (above 90%) validated in real scenarios	KPI3.2 Facilitate deployment of blockchain technologies by non-cybersecurity experts in Cybersecurity training sessions with, at least 20 participants	KPI3.3 Interoperability with at least one eIDAS identity schema	KPI3.4 Enable, at least 3 multiple simultaneous identification approaches for persons
Validation scenarios supporting KPI validation	A2#1	Not applicable[8]	A1#1, A2#1, C1#1	A2#1
Objective #4 Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust (CoT)	KPI4.1 Enable federated AI mechanisms for, at least three, heterogeneous devices and entities	KPI4.2 Enhance robustness of AI models for trust and security management by a factor of 30% in real scenarios	KPI4.3 Enable detection of anomalous behaviour with accuracy of 90%	KPI4.4 Availability of trust evaluation models for heterogeneous entities (devices, services, persons)
Validation scenarios supporting KPI validation	A6#1, A7#1, C5#1, C6#1, C7#1	NA[9]	A6#1, B4#1, C6#1, C7#1	Validation scenarios involving Reputation System
Objective #5	KPI5.1	KPI5.2	KPI5.3	

[8] In scope of training activities (T5.6)
[9] Evaluation performed in scope of WP3

Provide a hardened encryption with recovery ability	Provide at least three encryption mechanisms with low overhead	Enable efficient encryption with Root of Trust (RoT) information	Support selective recovery ability in encryption mechanisms: who and what can be recovered	
Validation scenarios supporting KPI validation	Validation scenarios involving eSIM-based (A2#1-A7#2, C2#1-C7#2) and cryptochip-based hardened encryption (B1-B6)	Validation scenarios involving eSIM-based (A2#1-A7#2, C2#1-C7#1) or cryptochip-based HE (B1-B6)	A6#1, A7#2, C5#1	
Objective #6 Self and coordinated healing with reduced human intervention	KPI6.1 Recovery, at least 95% of the system functionalities prior to anomalous behaviour	KPI6.2 Support coordination of recovery to pre-defined trust levels	KPI6.3 Reduce human intervention to the strictly required, in healing and recovery procedures	
Validation scenarios supporting KPI validation	A6#1, A7#2, C5#2	A6#1, A7#2	A6#1, A7#2, C5#1, C6#1, C7#1	
Objective #7 Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory	KPI7.1 Promote sharing of IoT threat data in EU, respecting privacy and data regulations	KPI7.2 Enable a novel automated and privacy-preserved CTI approach exploiting the European MISP platform (MISP4IoT)		
Validation scenarios supporting KPI validation	A6#1, C6#1, C7#1			

The following sections provide further details regarding the achievability of the objectives and KPIs listed in Table 24.

5.3.1 Objective #1

"*To create a decentralized framework for IoT systems - ARCADIAN-IoT framework*"

ARCADIAN-IoT has developed a robust decentralized security framework for IoT systems, building on the following key aspects:

Identity Management Plane: Decentralized Identifiers (DIDs) provide a way for end-user stakeholder organizations to cryptographically prove their ownership of credentials. This ensures a high level of security and control over identity-related information.

Trust Management Plane: Verifiable Credentials enable various entities to issue credentials,

leading to a decentralized, self-sovereign identity approach. This means that actors such as national bodies and organizations can issue credentials to individuals and IoT devices, enhancing trust in the ecosystem. Additionally, the Reputation system publishes reputation information in a decentralized manner on the Permissioned Blockchain to enhance transparency and security.

Common Plane: The use of Permissioned Blockchain facilitates distributed and decentralized storage for publishing information across different planes. This allows for secure storage and sharing of data, such as cryptographic key information for Hardened Encryption and Decentralized identifiers, as well as Reputation information. The deployment of the Publisher Smart Contract on multiple peer nodes ensures redundancy and resilience.

In summary, ARCADIAN-IoT's decentralized framework offers a comprehensive solution for security and trust in IoT systems, leveraging innovative technologies such as DIDs, Verifiable Credentials, and a Permissioned Blockchain to publish security information such as Reputation.

5.3.2 Objective #2

"***Enable security and trust in the management of objects' identification***"

Associated KPIs:

- **KPI2.1** Support, at least, two identity approaches at hardware level (SIM and CryptoChips).
- **KPI2.2** Avoid single trusted entities through decentralized approaches (SIM identity approach).
- **KPI2.3** Support, at least two robust identity mechanisms for devices and apps/services.

The work performed to achieve this objective includes the research performed for supporting the different IoT object identification methods. On one hand, **Decentralized Identifiers** and **Verifiable Credentials** identification methods follow the Self-Sovereign Identity approach, and provide: a) two **Decentralized Identifiers** methods for IoT Devices (DID:WEB & DID:PRIV) as suited to their use cases, where the latter leverages the **Permissioned Blockchain** as trust anchor for published Decentralized Identifier Documents b) **Verifiable Credentials** based on Hyperledger ARIES GO framework is provided by the ATOS SSI solution Ledger uSelf, which is extended to support IoT Devices in the ARCADIAN-IoT framework.
Regarding the **crypto chip**, supporting constrained IoT Devices, these were not able to support Verifiable Credentials and Decentralized Identifiers directly due to their heavy cryptographic computations, and so an IoT GW solution was implemented to provide a simpler Challenge / Response DID Authentication on behalf of the constrained IoT Devices. Regarding verifiable credentials, a unique Device ID is implemented within GMS IoT Device firmware and Middleware, together with its correlated user and password, to strengthen the authentication phase.
Regarding the contributions of **SIM**-related technology for this objective, these have been multi-fold. In what regards KPI2.1, a technology based on SIM identification credentials and authentication processes was developed to provide a zero-touch mechanism to authenticate IoT devices to Cloud services. This technology was integrated within ARCADIAN-IoT Multi-Factor Authentication. Regarding KPI2.2, a process based on GSMA IoT SAFE was developed, where the SIM digitally signs encrypted payloads, identifying their source. The private/public keys used for the digital signatures are generated in a decentralized manner, in the SIM hardware secure element of each IoT/consumer device. Regarding KPI2.3, for ensuring that only authorized apps access the SIM (e.g., are able to request digital signatures), a process for including the partner apps identification in the SIM secure element was implemented, so that the mobile operating system could allow only those apps to access it. Moreover, HTTP signature was used for service identification by ARCADIAN-IoT framework.
For supporting the simultaneous use of multiple authentication factors, a **Multi-factor Authentication** (MFA) component was developed. This component orchestrates the several identity credentials used in the project, for devices and for persons, issues signed and protected ID tokens, and informs security components of authentication events, allowing to infer related threats.

5.3.3 Objective #3

"***Enable distributed security and trust in management of persons' identification***"

Associated KPIs:

- **KPI3.1** High accuracy in facial recognition AI models (above 90%) validated in real scenarios.
- **KPI3.2** Facilitate deployment of blockchain technologies by non-cybersecurity experts in Cybersecurity training sessions with, at least 20 participants.
- **KPI3.3** Interoperability with at least one eIDAS identity schema.
- **KPI3.4** Enable, at least 3 multiple simultaneous identification approaches for persons.

The implementation of the **Biometrics** component has progressed to ensure that personal data only occurs for individuals giving explicit consent, given that facial data fall within the special categories of personal data regulated by article 9 of the GDPR. The research work on facial verification has focused on far-range distances (more than 2 meters from the camera), enabling the verification from drones, and close-range distances (less than 2 meters from the camera) covering verification from the smartphone with a total accuracy of 91.65% and reducing the False Acceptance Rate to less than 0.5% - which enables the fulfilment of *KPI3.1*.
Hyperledger ARIES GO framework is provided by the ATOS SSI solution Ledger uSelf, which is extended to support Organisation Members in ARCADIAN-IoT framework, in addition to existing support for Persons.

The Self-Sovereign Identity solution provides an SSI Wallet app, SSI Broker and Agent for issuing and verifying Verifiable Credentials and also a Mediator to support end user authentication to a mobile device. The SSI solution is built on the ATOS Ledger uSelf and supports one **Decentralized Identifier** method (DID:PEER) and b) Person & Organization Member **Verifiable Credentials.** With respect to meeting *KPI3.3*, ARCADIAN-IoT issues person eIDs following the specification of EBSI natural person schema[2] that is aligned with the eIDAS minimum data set. The aim is to make ARCADIAN-IoT identity claims interoperable with the future EU Digital Identity Wallet (EUDIW) when it is deployed as part of the new eIDAS 2.0 framework[3].

In the scope of *KPI3.2*, training was given on the deployment of chain code on a Hyperledger Fabric blockchain network.

The **Network-based Authentication** technology, which uses SIM credentials to authenticate devices in third-party Cloud services, is also applied to accomplish KPI3.4. This technology identifies the person though something that is expected that the person has, e.g. its smartphone, being another factor in ARCADIAN-IoT **MFA**.

The **MFA** contributed to the KPI3.4 by combining the 3 multiple simultaneous identification approaches, specifically the (SIM-based) network identifiers, biometrics, and SSI, and issuing, as result, a signed and protected ID token for the authenticated operation (of persons in the case of this objective).

Additionally, support is provided by ATOS, for Onboarding all the different entities in the IoT ecosystem (Persons, Organization Members, IoT Devices & constrained IoT Devices) to the ARCADIAN-IoT framework and linking them with the creation of an aiotID through the implementation of an SSI IdP, under the **Verifiable Credential** component.

5.3.4 Objective #4

"***Provide distributed and autonomous models for trust, security and privacy – enablers of a Chain of Trust (CoT)***"

Associated KPIs:

- **KPI4.1** Enable federated AI mechanisms for, at least three, heterogeneous devices and entities.
- **KPI4.2** Enhance robustness of AI models for trust and security management by a factor of 30% in real scenarios.

- **KPI4.3** Enable detection of anomalous behaviour with accuracy of 90%.
- **KPI4.4** Availability of trust evaluation models for heterogeneous entities (devices, services, persons).

In the scope of the **Federated AI** component, based on the analysis undertaken on the state-of-the-art of privacy-preserving federated AI, a new data rebalancing model was defined and evaluated in a set-up with three heterogeneous clients which makes the data non-independent and identically distributed (non-IID). The empirical results show that the proposed data rebalancer can mitigate the issue of model degradation caused by the imbalanced and non-IID data, which is common in federated learning. Besides the data rebalancing algorithm, a robust and communication-efficient federated aggregation scheme has been designed as well. It accelerates the training process by resizing the models without degrading the performance. In addition, it enhances model robustness against adversarial attacks, such as data/model poisoning attacks and Byzantine attacks. The proposed scheme has been evaluated in different peer-to-peer federated setups including random networks where one or multiple adversarial clients are involved. The empirical results show that the proposed aggregation scheme is able to mitigate the effects caused by adversaries or malicious clients. Additionally, the proposed solution outperforms the other secure aggregation methods, such as Krum, Trimmed-Mean, and Median. Both two subcomponents have been tested and evaluated with real-world datasets and results indicate the fulfilment of *KPI4.2*. In addition, Federated AI is employed in ARCADIAN-IoT components such as the **Device Behaviour Monitoring** and **CTI** system, contributing towards *KPI4.1*. For IoT device intrusion detection capabilities of **Device Behaviour Monitoring**, the training of models has been performed, as well as initial evaluation activities comparing against considered baseline results. As its ML models can now detect anomalous behaviours with an accuracy of approximately 96%, it is considered that *KPI4.3* is fulfilled.

Regarding the IoT network protection, the implementation of the cognitive loop – involving **Network Flow Monitoring**, **Self-Healing** and **Network Self-Protection** – for the detection and mitigation of known cyber-attacks in the Edge and Core segments of the IoT network has been progressing, resulting in an initial deployment of the cognitive loop to protect the third-party services from attacks initiated on the Internet. Regarding the distributed and autonomous trust modelling, **Reputation System** builds the reputation of a given entity (e.g., person, device or IoT service/app) according to the information retrieved from events, contributing to *KPI4.4*.
Three reputation models have been designed and implemented: 1) Alpha-beta model, 2) the prioritized Alpha-Beta model, 3) and Dominance Model. The first two models are applicable to all types of entities, while the dominance only applies to persons. The prioritized Alpha-Beta model considers the events' severity information, which can impact the reputation score more quickly. For instance, to reset the reputation score when the severity of events is high.
As stated in Objective 1, the reputation system also stores the reputation scores in the **Permissioned Blockchain**.
The **Network-based Authorization** supports and relies on the trust evaluation models (KPI4.4) to enforce trust communication policies in the cellular core network. It also distributes the trust information to the devices SIM, so that this hardware can enforce trust-based self-protection and self-recovery processes.
Finally, the **Remote Attestation** system, targeting the assessment of IoT device trustworthiness, has been implemented and integrated with the Hardened Encryption for ensuring claims/evidence confidentiality and their selective decryption according to the target verifier(s), having been validated in smartphone devices. The attestation results (or outcomes) are also used to provide the **Reputation System** with valuable trust indicators regarding the IoT devices, contributing to the Chain of Trust.
To further contribute to this objective, the Chain of Trust has been specified, clarifying the different components from ARCADINA-IoT's horizontal and vertical planes which contribute to the CoT (e.g. providing a Root of Trust or leveraging it to build trust).

5.3.5 Objective #5

"***Provide a hardened encryption with recovery ability***"

Associated KPIs:

- **KPI5.1** Provide at least three encryption mechanisms with low overhead.
- **KPI5.2** Enable efficient encryption with Root of Trust (RoT) information.
- **KPI5.3** Support selective recovery ability in encryption mechanisms: who and what can be recovered.

To address this objective and enable the availability of encryption and decryption mechanisms across all ARCADIAN-IoT framework, the implementation of **Hardened Encryption** libraries for encryption/decryption of data at rest, key management using Attribute-Based Encryption (ABE), and development of a Cryptochip have been undertaken; the usage of RoT information by leveraging UICC / **SIM** as secure element relied on GSMA IoT SAFE specification as baseline. The approach consists of using the SIM RoT for digitally signing data encrypted in the device with the ABE. Were developed middleware's to allow this technology to be used in Linux-based IoT devices and in (Android) consumer devices, which allowed to validate it with all Domain A and Domain C IoT solutions' devices.
Regarding the development of ABE libraries for encryption and decryption, the core implementation with API in Go, Python, Java and C have been provided and tested on multiple devices. They support two encryption schemes, both based on the ABE paradigm. APIs for JavaScript are currently in development. Together with **cryptochip**-based encryption, these mechanisms fulfil *KPI5.1*. Moreover, the first version of **Hardened Encryption** Key management has been provided for the mentioned mechanisms.
As for the **cryptochip-based Hardened Encryption**, the usage of RoT **information** by leveraging the crypto chip as secure element has been validated. This one is a consequence of the manufacturing chosen vendor architecture (Infineon, a top cyber security contributor) and a consequence of the way how was implemented into end-to-end solution, to mitigate bith (grid domain particularities, the micro controller base devices (by embedding the encryption and decryption function into device firmware) and the interface with IoT platforms (by TLS interfacing). Into this end-to-end solution, BOX2M used the best practices recommended by Infineon (mainly related to cloud base component, the Middleware, as encryption and decryption component, closing the communication path with device in all operations lifecycle stages of this one).
Finally, the selective recovery ability leveraging the results of **Hardened Encryption** to secure the backups has been integrated into **Self-Recovery** component – addressing *KPI5.3*. Moreover, to provide layered access policies to different level users, **Hardened Encryption and Self-aware data privacy** components have been combined and integrated (and demonstrated in Domain C) to ensure data confidentiality and privacy with at least one encryption algorithm – plus anonymisation and another encryption algorithm were individually implemented and tested within the Self-aware data privacy component.

5.3.6 Objective #6

"***Self and coordinated healing with reduced human intervention***"

Associated KPIs:

- **KPI6.1** Recovery, at least 95% of the system functionalities prior to anomalous behaviour.
- **KPI6.2** Support coordination of recovery to pre-defined trust levels.
- **KPI6.3** Reduce human intervention to the strictly required, in healing and recovery procedures.

With respect to recovery of IoT devices (and associated data or services), the support of the **Self-Recovery** mechanisms for fast recovery of data and services after incidents has progressed as follows: upon events such as anomaly or intrusion detection in IoT devices – which may result from known or unknown attacks - and the enforcement of protection policies (e.g., protection policies applied by the **IoT Device Self-Protection**), device's data or service recovery actions can be performed. Two steps have been established in the recovery phase, the first being the

recovery of credentials and the second being the recovery of data and services - both enabled by advanced cryptographic algorithms (e.g., functional encryption and secure multi-party computation) as needed. Different keys will be distributed to different stakeholders, by which different levels of data will be able to be decrypted. The authorization for a device to access the recovery services will be based on its reputation score (e.g., the IoT application, upon being informed about the device's compromised security, will decide on the need to go through the process of **Credentials Recovery.** A dedicated Credential Recovery server is implemented for the SSI Wallet where an end user registers their email and provides a secret password used to encrypt the SSI Wallet´s credentials to make backups and access recoveries. For IoT Devices, Credential Recovery is based on rotation of the device´s SSI Agent public keys on the Permissioned Blockchain and re-issuing the device fingerprint claims as its Verifiable Credential. The contributions mentioned in previous Objectives regarding the **Device Behaviour Monitoring** (AI-based intrusion detection), and the aforementioned chaining between **IoT Device Self-Protection** and **Self-Recovery** both contribute to *KPI6.3*, for incidents detected at the IoT device. The **Credentials Recovery** and **Self-Recovery** is aimed at enabling *KPI6.1* – the achievable recovery degree is above 95% for both the components. Moreover, in case of full recovery and re-onboarding of IoT devices after incidents, the Reputation System is able to recompute the trust / reputation level – based on evidence regarding the state of the device collected by Remote Attestation and according to the policies of the IoT service provider and/ or device manufacturer. From the IoT network infrastructure point of view, the network monitoring (via **Network Flow Monitoring**) for detecting malicious flows in real-time has been validated, as well as the ability to trigger healing actions i.e., mitigation of network anomalies (via **Network Self-Healing**) and protection actions, i.e., enforcing protection rules at the data plane deemed necessary for safeguarding the infrastructure, IoT devices and services against volumetrics attacks (via **Network Self-Protection**). A DDoS attack was launched through an emulated 5G infrastructure where the self-protection cognitive loop successfully detected, coordinated and mitigated the thread, healing without human intervention in every segment and service of the network. These contributions directly address *KPI6.3* for incidents detected at the network side.

5.3.7 Objective #7

"*Enable proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory*"

Associated KPIs:

- **KPI7.1** Promote sharing of IoT threat data in EU, respecting privacy and data regulations.
- **KPI7.2** Enable a novel automated and privacy-preserved CTI approach exploiting the European MISP platform (MISP4IoT).

The **CTI** system in ARCADIAN-IoT framework is an extension of the popular open-source CTI platform MISP and implements IoC-specific functionalities, such as support for the new formats *tinySTIX* and *tinyTAXII*, as well as FL/ML models for IoC ranking, event classification, and IoC clustering. Also, the CTI system can process events regarding detected anomalies or intrusions both originating from the network (from the **Network Flow Monitoring** and **Network Self-Healing**) and IoT devices (from the **Device Behaviour Monitoring**). This set of new features collectively addresses KPI7.2. Additionally, the **Federated AI** component integrated into the CTI system enables the sharing of IoCs for collaborative model training, addressing KPI7.1. Finally, the **Device Behaviour Monitoring** is able to issue Indicators of Compromise which are able to be processed by the IoT Device Self-Protection, Reputation System, and Cyber-Threat Intelligence. These activities jointly contribute to *KPI 7.1*.

6. LEGAL COMPLIANCE ANALYSIS

6.1 Overview of Legal Considerations

As already noted in the previous deliverables, the design of such technologies, the interaction of them potentially raises legal compliance questions and potential risks, which are specifically regulated by European regulation (hereinafter, the "**Regulatory Framework**").

In particular, the main legal considerations have been identified in relation to the compliance of data protection legislation, as provided in the Regulation no. 679/2016 ("**GDPR**"), as well as the possible implications in using components that are based on artificial intelligence, considering the recent approval of the European regulation on artificial intelligence ("**AI Act**").

Starting from the identification of Domain legal concerns (*infra*, par. 6.2.) and the Regulatory Framework (*infra*, 6.3.), to follow a specific methodology, in this section, a final legal compliance assessment of the Project is reported (hereinafter, the "**Assessment**").

6.2 Domain Legal Concerns

Among the Domains and the related use-cases, some legal concerns have been identified, in relation to the use of personal data processed in order to offer services, while using new technologies, such as AI, Facial recognition, blockchain and IoT. For that reason, in the previous deliverable D5.4., the main legal concerns were identified, in relation to each domain.

6.2.1. Domain A

Domain A has appeared to be the most critical one, due to the use of drones and facial recognition, and technologies such as AI and IoT, that, under a legal perspective, must comply with the Regulatory framework. In particular, the drone operations must be carried out with the minor impact and interference with privacy and data protection of individuals, especially if an AI system is integrated, as a component, in the drones, in order to carry out the related activities (that, in this case, consist in the facial recognition of the user).

The main legal concerns of the Domain A can be summarized as follows:

- ***Biometric Identification and recognition process***: the correct classification of the facial recognition process carried out by the drones, taking into account the risk of involving other people than the one to be identified, among the following ones: real-time biometric identification system; remote-biometric identification system; post biometric identification system;
- ***Mass surveillance issue***: in light of the identification of biometric identification process, the verification if a potential mass surveillance activity is carried out;
- ***AI involvement***: dealing with the risks related to the use of AI systems, including the lack of comprehensive and transparent information on how the technologies work, as well as, the lack of human intervention and control in the automated process; moreover, the ones related to the technical robustness of the AI systems, the confidentiality of the data processed and the non-discrimination/fairness of data processing;
- ***GDPR principles compliance***: ensure the compliance with the principles of the GDPR, such as data minimization principle, full transparency information, security and adoption of technical and organizational measures and accuracy of the data;
- ***Consent for processing biometric data***: request a valid consent to process the biometric data, as provided by the Article 9 (a) of the GDPR; The acquisition of consent must comply with the prerequisites of the GDPR, such as informed, free, specific, and unequivocal, with respect to the Article 7 of the GDPR.

6.2.2. DOMAIN B

Domain B, related to grid infrastructures, does not present any specific issues under a legal perspective; specifically, none of the data protection issues have been identified, since, as reported by the Partner, personal data will not be involved.

6.2.3. DOMAIN C

Also, Domain C has appeared to be critical considering that the major risks occurred using a medical IoT system.

The main legal concerns of the Domain C can be summarized as follows:

- ***AI involvement****:* dealing with the risks related to the use of AI systems, including the lack of comprehensive and transparent information on how the technologies work, as well as, the lack of human intervention and control in the automated process; moreover, the ones related to the technical robustness of the AI systems, the confidentiality of the data processed and the non-discrimination/fairness of data processing;
- ***IoT System involvement****:* dealing with the risks related to the use of sensors to monitor the patient, including the inaccurate (even false) data about the subject. Moreover, 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;
- ***GDPR principles compliance***: ensure the compliance with the principles of the GDPR, in particular with attention to the possible lack of control and information for the data subject (i.e., the subject whose data is processed by the IoT system), as well as the repurposing of original processing, in particular while processing health-related data, which therefore fall into the special categories of personal data under Article 9 of the GDPR;
- ***Consent for processing health data of the patient****:* requesting a valid consent to process health data, as provided by Article 9 (a) of the GDPR. The acquisition of consent must comply with the prerequisites of the GDPR, such as informed, free, specific and unequivocal (see Article 7 of the GDPR);
- ***Protection of minors****:* ensuring a particular standard of protection in case minors are involved in the use of AI/IoT technologies, pursuant to the prerequisite of Article 8 of the GDPR;
- ***Rights of the data subjects***: ensuring that the rights of the patients, such as, the right of deletion of their data could be exercised in a free and easy manner.

6.3 The Regulatory Framework

The relevant legal framework for this deliverable is the Regulation (UE) 2016/679 on the protection of natural persons regarding the processing of personal data and on free movement of such data ("**Regulation**" or the "**GDPR**"), as well as the other provisions adopted by the competent authorities' European authorities and bodies, namely:

- the Opinion 8/2014 on the "Recent Developments of the Internet of Thing" of the Article 29 Data Protection Working Party (now, the European Data Protection Board, "**WP29**" or "**EDPB**");
- "White Paper on Artificial Intelligence" of the European Commission;
- "Ethics Guidelines for Trustworthy Artificial Intelligence" adopted by the High-Level Expert Group on Artificial Intelligence set up by the Commission;
- 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;
- Directive 2002/58/EC concerning the processing of personal data and the protection of

privacy in the electronic communications sector (Directive on privacy and electronic communication or "**e-Privacy Directive**");
- Guidelines 3/2019 on processing personal data through video devices, and Guidelines 2/2021 on Virtual Voice Assistants of the EDPB, which contain indications on the processing of biometric data for the automated, unique identification of users;
- European Union's Artificial Intelligence Act (AI Act), in its latest version adopted by the Parliament ("**AI Act**")
- European Health Data Space.

Considering that, on one hand, the AI Act has recently been approved by the Trilogue and will come into force, after the end of the Project, in the context of final Assessment, some of the main aspects related to the AI regulation have to be mentioned, to provide useful guidance in a possible exploitation of the Project technologies. On the other hand, also the European Health Data Space has been, at the present time, only approved by the European Parliament and, after the final approval and the coming into in force, the framework will deal with several and important issues related to the use of health data for research, innovation, and decision-making.

It is worth to be mentioned that the AI Act recalls the ethical principles developed in 2019 by the "High-Level Expert Group on Artificial Intelligence" appointed by the European Commission, in particular: **human agency and oversight**, which means that AI systems are developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans and, **transparency,** means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights.
Moreover, the AI Act applies to providers, deployers, importers and distributors, Section 3 sets out a series of **obligations** intended for each of these categories. The main obligations (Art. 16), imposed on providers of high-risk AI systems, are: to **ensure** that their high-risk AI systems comply with certain requirements listed in Section 2 (e.g., to adopt risk management systems or to design and develop the system in such a way as to provide sufficient transparency for *deployers* to interpret the various *outputs*); to **indicate** on the high-risk IA system name, registered trade name or trademark, and address at which they can be contacted; to **have** a quality management system in place (Art. 17), e.g., a document ensuring AI Act compliance); to **keep** documents (Art. 18): e.g., the supplier must keep technical documents, those related to quality management systems and EU compliance; to **prepare** an EU declaration of compliance (art. 47); to **take** corrective action (e.g., withdraw, disable) if they believe that a high-risk AI system they placed on the market or put into service is not in compliance with the AI Act; to **provide** the competent authorities with all requested information and documentation. Also, the AI ACT provides some other obligations to **deployers** (or users) of high-risk AI systems, for instance: to **take** appropriate technical and organizational measures to ensure compliant use; to **entrust** human oversight of the systems to suitably competent individuals; to **monitor** the operation of the systems and, where appropriate, inform providers of any malfunctions; to **cooperate** with relevant supervisory and control authorities as necessary; to **conduct**, in the cases provided for in Article 27, an assessment of the impact on fundamental rights that such systems must respect.

In any case, developing an AI System the following obligations must be considered: **prepare and keep up-to-date technical documentation** of the model, including the training and testing process and the results of its evaluation; **Implement a policy** aimed at complying with Union copyright law; **cooperate** with the Commission and the relevant Authorities.

However, as far as what the development of this project specifically is concerned, the AI Act states specific provisions concerning the systems that are capable of **biometric data processing**. Indeed, the AI Act aims to establish a comprehensive regulatory framework to ensure the responsible and ethical use of such data, and inevitably triggers the application of the GDPR.

Specifically, the Act sets out requirements for transparency, accountability, and fairness in the processing of biometric data by AI systems.

Firstly, at recital n. 8, the AI Act provides a "functional" definition of biometric identification systems, as "an AI system intended for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviours simultaneously to significantly facilitate the identification of natural persons without their active involvement".

Recital n. 8, then, offers a distinction between "real-time systems" and "post" systems. "Real-time" remote biometric identification system means systems whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay.
This comprises not only instant identification, but also limited short delays in order to avoid circumvention; in the case of "post" systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

Given this distinction, the AI Act considers "real-time remote biometric identification systems" such as "high risk AI system". In fact, the AI Act adopts a risk-based approach to regulate the deployment and use of artificial intelligence technologies within the European Union. This approach aims to assess the potential risks associated with AI systems based on their intended use and impact on individuals and society. By categorizing AI applications into low, high, and unacceptable risk levels, the Act aims to provide fair protection for every possible outcome.

Specifically, the Article 5, lett. d) of the AI Act prohibits the use of the aforesaid "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following **objectives**:

1. the targeted search for specific **victims** of abduction, trafficking in human beings and sexual exploitation of human beings as well as search for missing persons;
2. the **prevention** of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
3. the localisation or identification of a person **suspected** of having committed a criminal offence, for the purposes of conducting a criminal investigation.

6.4 ARCADIAN IoT Legal Compliance Considerations

Taking into account the Domain legal concerns outlined at an earlier stage of the project, a methodology has been adopted (hereinafter, the "**Methodology**") to monitor the implementation and development of the technologies and, by the end, to evaluate the compliance of the project with the Regulatory Framework (*infra* 6.3.*)*.

In particular, the Methodology consists in the following actions:

- active participation in workshops and/or calls organized by the Domain Owner to follow and monitoring properly the development of the technologies;
- supporting the development phase of all the project's technologies through a privacy-by-design approach to identify critical aspects (*infra);*
- drafting of templates to ensure compliance of any obligation provided for by the Regulatory

Framework;
- responses to questions could have substantially impact from a legal standpoint;
- submission of a legal checklist (hereinafter, the "**Checklist**"), with specific questions for Domain Owner, with the aim of considering whether the final implementation of the technologies - and the possible future exploitation - fully complies with the Regulatory Framework (*see [11] - section E*).

The Checklist is composed of three sections related to each Domain, which can be divided, ideally, into two main parts based on the topics dealt with.

The first part of the Checklist is about the general questions aimed at understanding which and how the data will be exchanged, as well as whether the implemented technology meets the standards outlined in the Regulatory Framework as mentioned before.

The second part, addressed to the Domain Owner, is indeed divided into three subsections for each Domain and the related use cases. The aim of the questions is to collect relevant information on how the processing of personal data in the context of the use-cases, considering the Domain legal concerns, as well as the risks and the implications of using the AI. The analysis of the answers is offered below and were fundamental to carry out the Assessment of the Project.

6.4.1. Domain A

As known, Domain A implements a **Drone Guard Angel (DGA) service**, the use-cases related to this domain aim to ensure the authentication of an individual in an emergency situation, through drones and AI systems.

6.4.1.1. Checklist Results

Through the Checklist, some relevant information has been acquired.

- **P1/P2:** first, in the development of P1 and P2, in Domain A, personal data of the volunteers were only collected with their consent, and the processing is only related to the test stage of the DGA service and will not be shared outside the Project. Indeed, the images collected by the drones are only about the test phase/laboratory phase. In case of exploitation, see further indications *infra.*
- **Collection of data and consent of the user:** the data collected in the phase of registration are the ones essential for the use of the DGA service; the data are stored, but the user can exercise their rights to deletion and rectification. In other words, the DGA service collects and stores personal data in order to enable user registration and related app operation, before acquiring the user consent. A pseudo-ARCADIAN-IoT ID (called "aiotID") is generated for each registered entity and associated with the e-mail address. The above-mentioned process ensures the total control of the users of their data, and, for that reason, it can be considered compliant to the GDPR;
- **AI training systems:** the databases used to train the AI systems, also in relation to the Federation AI system and the device behaviour monitoring, were identified and documented by the Partners in the D3.3. and D4.3. In particular, the name/code, identification version and date of creation were precisely identified. All the codes used to train the model and the components are published in the Project Gitlab repository. Moreover, as explained more precisely in the D7.7., all the AI components were trained with databases in which the data related to different ethnicities, gender and age, were collected and used, in order to reduce the risk of bias by the algorithms;
- **AI developed component:** the result of the development of AI components can guarantee the integrity, (also of the classification of the system call traces) due to the reduction of the biases and the improvement of the robustness of the AI model. In this

latter case, for instance, in case of data interference of devices, due to the quantities too much elevated of data, the robustification mechanism manages data rebalancing. Moreover, the AI system has been developed in order to be supervised easily by human beings and the auditing activity;

- **Biometric process:** the DGA, in order to provide its service, does not conduct, among the different typologies of biometric identification processes, any of the identification processes. Instead, the DGA conducts a different process, called "remote biometric verification system". For that reason, there is no process that allows the identification of the user, but only the match between the image collected in the registration phase and the image captured by drone. So, an identification is processed. No emotion recognition systems have been implemented.

6.4.1.2. Conclusions and Recommendations

Analysing the Checklist answers noted above, along with the findings from the previous Deliverable D5.4 on the Domain legal concerns about potential critical issues, as well as the Deliverables mentioned by the Participants partners, the following conclusions can be drawn from a final Assessment perspective.

Firstly, the DGA service allows only a **remote biometric verification process.** For that reason, the difference between the remote biometric identification and verification systems is crucial.

A remote biometric identification system is defined as an AI system intended **only** for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the specific technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviours simultaneously to significantly facilitate the identification of natural persons without their active involvement.

In the case of ARCADIAN-IoT, on the contrary, the process is only based on a verification which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity for having access to the service (i.e. to request the drone, to be actively protected and rescued).

However, the potential risks involved in using a remote biometric process were taken into account, also to the ones that - normally - are only applicable to the remote biometric identification processes. Indeed, in the cases of remote biometric identification processes, those may be used for the processing of the biometric data of a large number of persons without their active involvement. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay.

Considering that, in developing the DGA service, the following relevant **aspects** were considered in order to reduce the potential **risks** and the related **impact**:

- in the DGA service, the process has been developed to take as little time as possible to perform the comparison and the identification of the person – in a normal public 4G/5G connection this process should not take more than 10 seconds.
- the service can be used only in situations of extreme urgency and for safety and emergency purposes. Indeed, only the minimum necessary data are collected during all the process of the biometric identification.
- on the development of the process, appropriate safeguards have been identified during specific use-cases dedicated to security, also of data.
- considering the specific functioning of the DGA Service, a mass surveillance process is

impossible to be carried out, for several reasons: first of all, the record of the drone is not stored and, so, the identification of people other than the user that has requested the service could not be performed; secondly, the drone has only a short autonomy – both in time and traveling distance.

Indeed, in relation to this aspect, in the context of the Assessment, it is considered that specific measures that are capable of reducing the impact in the use of the drone in relation to the individuals that can be involved have been taken. Indeed, the drone operations, as described, are carried out with 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.
In any case, the recommendation is that, in a future exploitation of the Project, national frameworks must be taken into account, in order to verify any possible contrast to the public security laws.

For the other Domain legal concerns, the Assessment can be compliant with the Regulatory Framework, in relation to the GDPR principles, especially to the data minimisation. Moreover, the risk that a bias (unconsciously set by the programmers or developers) negatively influences the AI result has been considered and appropriate safeguards have been identified and adopted. The same could be said about the opacity of the algorithm and the measures taken to guarantee a rightful explainability of the algorithm.

In case of **exploitation** of the DGA Service, some **recommendations**, under a privacy perspective, as well as the utilisation of AI components need to be followed:

- pursuant to article 13 and 14 of the GDPR [9], a privacy policy must be provided, in the moment of the registration in the APP (so, in the moment in which the user fills the form with his or her data). The privacy policy must contain: the identity of the organisation processing data; the purposes for which the data is being processed; the type of data that will be processed, the right to withdraw the given consent; how to exercise the data subject rights;
- an informed, specific and explicit consent for the processing of an individual's image has to be given by the user, at the moment of the registration in the DGA app:
- the user must be aware of the data processing, especially because, in case of the use of the DGA Service, a remote biometric identification process is carried out, also including the use of AI components and systems.
- at the registration in the DGA Service, the user must also receive the terms and conditions of the APP, which explains the rules related to the access and use of the DGA Service. The Terms and Conditions must contain the following information: the use of the DGA service; the means of the registration on the DGA App for requesting the service; how the account is created and can be used by the user; the use of personal data, referring also to the content of the aforementioned privacy policy; the duration and termination; warranties and limitations of liability; cost of the services (if any) and means of payment; intellectual property; governing law and jurisdiction.

6.4.2. Domain B - Grid Infrastructure Monitoring

Domain B develops an IoT solution for monitoring grid infrastructures allowing grid operators to obtain an accurate perception of the grid operation and potential issues.

6.4.2.1 Checklist Results

Domain B does not present specific data protection issues, since it does not involve personal

data, but only aggregated data, completely disjointed from the subject.

In the Checklist, it was only confirmed that when utilising the Grid infrastructure systems developed by ARCADIAN-IoT, the Device Behaviour Monitoring, Reputation System, Self-Aware Data Privacy and Remote Attestation process only device-specific information (not associated with personal data).

6.4.2.2. Conclusions and Recommendation

In this context, considering the disclosures provided on several occasions (see the methodology used), this Domain and the related technology does not have apparently any specific critical issues, due to the absence of personal data processing. In the case of exploitation, the aspect that needs the most attention is the use of the best techniques of pseudonymization and anonymization of data. The recommendation is to follow the guidelines of Data Supervisory Authorities, the European Data Protection Board and the other European Authorities on the application of those techniques to personal data, to be sure to achieve the minimization of the impact on the data subjects involved.

6.4.3. Domain C - Medical IoT

The Domain C develops an IoT system, via body sensor networks, that enables home monitoring of patients.

6.4.3.1. Checklist results

Through the Checklist, some relevant information has been acquired.

- **Collection and storage of user data:** the data collected during the phase of registration are necessary and pertinent for patient care, considering the data minimisation principle. The data encrypted is stored in a specific database as long as necessary for the purposes related to the service, including the fulfilment of legal obligations and, moreover, accounting and reporting purposes. The access to data is allowed only to the data subject and the doctor (and her/his staff) assigned to the patient and the data cannot be downloaded (unless the patient gives consent);
- **AI training systems:** the databases used to train the AI systems were identified and documented by the Partners in the D3.3. All the data sources and code used to train the model and their components are published in the Project Gitlab repository with commit dates. Also, the code is documented, readable, secure, low maintenance, and robust;
- **AI developed components:** the result of the development of AI components can ensure that the data used in algorithm training for the Pilot (and, in addition, in other activities related to testing and training) are not disclosed outside the ARCADIAN-IoT Project. From the perspective of integrity, no additional solutions are adopted to ensure integrity, as this is guaranteed by MISP by nature.
- **Technical measures:** appropriate technical measures have been taken to ensure the security of personal data, specifically encryption (Use case C3). In addition, technical measures are enhanced by the integration with components such as the **Device Behaviour Monitoring** (to detect abnormal device behaviour and anomalous authentication events) and other ARCADIAN-IoT integrated **Trust Components** (verifiable credentials, network-based authorization enforcement, Reputation system, and Remote attestation). The execution is logged and can be monitored by humans through logs and can be stopped at any time by admins.

6.4.3.2. Conclusions and Recommendations

Analysing the Checklist answers noted above, along with the findings from the previous Deliverable D5.4, on the Domain legal concerns about potential critical issues in this Domain, as well as the Deliverables mentioned by the Participants partners, the following conclusions can be drawn from a final Assessment perspective.

In the context of this Domain, the main risk in light of the Regulatory Framework is related to the use of IoT technologies in relation to the processing of data belonging to a special category, indeed health data (in other words, the so called “digital health”).

On the 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).

This issue was addressed in Domain C and the Assessment could be considered as positive. Considering that, the following relevant **aspects** were considered to reduce the potential **risks** and the related **impact**:

- the patients have total control of their data, including health-related one, and can exercise their rights (for instance, the right to erasure or the right to rectification of their data). Moreover, the data can be only visualised, and so, processed by the doctors that manage the care process of the patients. So, the Assessment can be compliant with the Regulatory Framework, in relation to the GDPR principles, in relation to the data collection.
- as for data used during the P1/P2-related activities, it belongs only to volunteers who have given their consent to participate and process their personal data. Furthermore, volunteers' personal data are not used for purposes other than those for which they were collected (i.e., the development of the Pilots).
- concerning specifically the health data, relevant technical security measures have been identified for ensuring a high standard of protection, due to the sensitive nature of this kind of data.

The Domain C does not raise concerns with respect to its concrete application. Nevertheless, in case of **exploitation** of Domain C, some **recommendations**, under a privacy perspective, as well as the utilisation of AI and IoT components have to be followed:

- pursuant to Article 13 and 14 of the GDPR, a privacy policy must be provided during the registration phase. The privacy policy must contain: how to collect, treat and manage personal health data of the patient in accordance with the Relevant Framework;
- under 9(2) (a) of the GDPR the legal basis for the processing of such categories of data can be found in the consent of the data subject, in accordance with the GDPR. Specifically, when the data processed concern minors consent must be given by the parental authority. For that reason, during the phase of registration and collection of patient data, it is necessary to acquire informed and explicit consent for the processing of the patient's personal data related to health conditions;
- the implementation of a data protection impact assessment (DPIA) on the health data processed with the IoT and AI systems, pursuant to Article 35 of the GDPR. Conducting a DPIA is strongly recommended, because it would provide a comprehensive picture of the circumstances of use of the technologies and the associated risks to the rights and freedoms of the individuals involved;
- pursuant to Article 17 and 20 of GDPR, the right to erasure and the right to portability must be guaranteed. The data subject has the right to obtain from the data controller the erasure of his or her personal data, and, in addition, the data controller must provide and transmit the personal data in a structure, in a commonly used and machine-readable format.
- when registering in the app, the user must also receive the terms and conditions of the APP, which explains the rules related to the access and use of the MIoT service. The

Terms and Conditions must contain the following information: the use of the MIoT service; the means of the registration on the for requesting the service; how the account is created and can be used by the user; the use of personal data, referring also to the content of the aforementioned privacy policy, in particular to the processing of health data; the duration and termination; warranties and limitations of liability; cost of the services (if any) and means of payment; intellectual property; governing law and jurisdiction.

6.5 Final Assessment Conclusions

In conclusion, it can be assumed that, in this second phase of the project and final prototype (P2), the use cases identified by the all the partners enabled the analysis of the most potential critical aspects related to the Project technologies. In particular, from a legal and data protection perspective, two core aspects were identified: (1) the processing of biometric data using a drone and, (2) the processing of health data thanks to IoT devices.

Throughout the design and implementation phase, all the partners have adopted and consistently retained an approach inspired by the principles of privacy by design and by default, in compliance with Article 25 of the GDPR, by paying particular attention to all those aspects that would - even potentially - have had legal, ethical, and data protection implications.

The adoption of this responsible approach, together with the use-cases designation, enabled the identification of the relevant countermeasures to be taken **to achieve the Project compliance with the Regulatory Framework**, especially regarding the said critical aspects.

Nevertheless, at a later stage of exploitation and market placement, some adjustments, also in line with the above recommendations, cannot be excluded and may be necessary in the light of the future approval and entry into force of the AI Act and European Health Data Space.

7. CONCLUSIONS

This document has reported the validation and evaluation activities (as part of Task 5.5), focused on the final prototype (P2) of ARCADIAN-IoT Framework. P2 (documented in D5.2) has substantially extended previous P1 prototype by integrating the full set of Security, Privacy, Identity, Trust and Recovery-enabling ARCADIAN-IoT functionalities, necessary for covering the complete set of IoT use cases. The validation and evaluation activities thus leverage the integration activities (in scope of T5.1), and the use cases implementation (in scope T5.2, T5.3 and T5.4, for each IoT application domain). All partners were involved in ARCADIAN-IoT framework's validation and evaluation activities, performed in the context of the 3 domains identified by the project.

The performed validation and evaluation activities have been organized and presented through three main technical vectors, for which some associated takeaways are presented:

(1) **technical validation of the framework against complementary (validation) scenarios**: Overall, the 20 established use cases and subsequent validation scenarios allowed the successful validation and verification of ARCADIAN-IoT innovative and interplaying capabilities.

(2) **technical evaluation of both the project-wide and component-specific KPIs**; the ambitioned capabilities have been reached through extensive implementation and integration work, necessary both for **supporting targeted environments** (i.e. Operating Systems or underlying hardware) and **to enable synergic added-value from previously inexistent interfaces**. Some examples include a) the inherent interplay between Security, Trust and Recovery features, allowing comprehensive IoT device, network and service monitoring for timely detection and response actions; b) the cooperation between Privacy and Security, as shown by the role undertaken by Federated AI for ensuring privacy-preservation across different ML-enabled security tasks such as anomaly detection of cyber-threat intelligence; c) the "Secure by Design" incorporation of (attribute-based) encryption across different types of security (e.g. attestation evidence) or sensitive data payloads (in this case further enhanced through privacy-ensuring data access policies).

(3) **legal validation**: the early consideration of critical legal and data protection aspects by the consortium, particularly a) the processing of biometric data using a drone, and b) the processing of health data through IoT devices, enabled the identification of proper countermeasures which support the project compliance with the regulatory framework. Future exploitation of the project results will nevertheless require revision in order to ensure alignment with evolving policies landscape (e.g. entry into force of AI Act, European Health Data Space).

From a wider perspective, some project-wide insights may be derived from the performed research, development, integration and validation activities, namely:

- inherently **decentralized mechanisms** such as DIDs, VCs and Blockchain can importantly support IoT ecosystems both by enabling Self-Sovereign approaches and supporting secure storage and sharing of (security-related data), being well-aligned with European values such as transparency, trust and security.
- **the exploitation of heterogeneous IoT context- and threat-awareness** (e.g. stemming from the Security Plane features) for **predictive cybersecurity**, while beneficial and aligned with **Zero Trust** paradigm, **must be strongly supported by non-contradictory and complementary policies stemming from all involved stakeholders** involved in the

supply chain (i.e. IoT service providers, device manufacturers, cybersecurity solution providers): this is particularly important for aspects such as the proper trust / reputation modelling of involved entities or an effective ability for enforcing credentials and self-recovery actions, calling for Autonomous (AI-based) **security orchestration able to enforce the multiple security requirements**.

- The early-on definition or clarification of the applicable **Chain of Trust**, building from unequivocal Roots of Trust and trust relationships, is mandatory for secure IoT deployments.

Summing up, the work performed during the project demonstrated that a decentralized, distributed and modular security architecture can successfully support and enhance the security in different IoT application domains, covering heterogeneous capabilities and constraints. Looking beyond ARCADIAN-IoT lifetime, new security components could be considered and added to cope with evolving threats (e.g. IoT and AI software supply chain attacks), extending ARCADIAN-IoT's architecture.

REFERENCES

[1] ARCADIAN-IoT, “D2.2 - Use case specification,” 2021”.

[2] ARCADIAN-IoT, “D2.5 - ARCADIAN-IoT Architecture,” 2022.

[3] ARCADIAN-IoT, "D5.3 - Use cases implementation", 2023

[4] ARCADIAN-IoT, "D5.4 - ARCADIAN-IoT Use Cases Validation and Legal Compliance", 2023.

[5] ARCADIAN-IoT, "D5.2 - Integrated ARCADIAN-IoT framework – final version", 2024

[6] ARCADIAN-IoT, " Grant Agreement number: 101020259 — ARCADIAN-IoT", 2021

[7] ARCADIAN-IoT, " D3.3 - Horizontal Planes, final version", 2024

[8] ARCADIAN-IoT, " D4.3 - Vertical Planes, final version", 2024

[9] Regulation ({EU}) 2016/679 of the Europea} Parliament and of the Council, 2016

[10] ARCADIAN-IoT, “D7.6: GEN - Requirement nº7”, 2022

[11] ARCADIAN-IoT, “D1.2 – Periodic Report – M36”, 2024 (to be released)

