Grant Agreement N°: 101020259

Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D5.4: ARCADIAN-IoT Use Cases Validation and Legal Compliance – 1st Version

Revision: v.1.0

Work package	WP 5
Task	Task 5.5
Due date	30/04/2023
Submission date	
Deliverable lead	IPN
Version	1.0
Partner(s) / Author(s)	IPN: Fernando Bastos, Paulo Silva, Sérgio Figueiredo UWS: Ignacio Martinez-Alpiste, Julio Diez-Tomillo, Jose M. Alcaraz-Claro, Qi Wang TRU: João Casal, Tomás Silva, Ivo Vilas Boas XLAB: Tilen Marc, Jan Antić MARTEL: Giacomo Inches, Andrea Falconi, Gabriele Cerfoglio BOX2M: Alexandru Gliga, Ovidiu Diaconescu, Marian Macoveanu RISE: Alfonso Iacovazzi ATOS: Ross Little RGB: Ricardo Ruiz LOAD: Pedro Colarejo E-LEX: Carmen Occhipinti, Adriana Peduto, Ariella Fonsi UC: Bruno Sousa

Abstract

This public report constitutes the deliverable D5.4 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 Case validation and legal compliance methodologies, specifications, and results for the first Prototype P1. The material presented in this document is the main outcome of **Task 5.5,** first version for P1, **(ARCADIAN-IoT Use Case Technical and Legal Compliance Validation)** and has considered inputs from 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). All technical partners were involved in the iterative process of methodology, validation specification and execution. Ultimately, this process will feedback the validation execution results contributing to an enhanced evolution of the framework integration activities and Use Cases implementation.

Keywords:

ARCADIAN-IoT Framework; Validation Specification; Technical and Legal Validation, Use Cases evaluation, Validation scenarios, KPIs

Document Revision History

Version	Description of change	List of contributors
V0.1	ToC and initial definition of contents	IPN
V0.2	First draft with introduction, methodology and scope for validation, evaluation and legal compliance	IPN, E-LEX, UWS, TRU, MAR, ATOS, LOAD
V0.8	Sections 1 to 6 mostly finalized	All partners involved
V0.9	Document with internal review	All partners involved
V1.0	Prepare document for 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	

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

EXECUTIVE SUMMARY

ARCADIAN-IoT framework proposes an integrated approach for managing identity, trust, privacy, security and recovery, across IoT devices, persons and services, relying on specialised 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 5.4 (ARCADIAN-IoT Use Cases Validation and Legal Compliance) - describes the ARCADIAN-IoT validation specifications and execution for the 3 Domain Use Cases available for the **first prototype P1**. It starts by introducing the Methodology and validation architecture to be used, Validation Scope (technical and legal) for P1 and KPI Evaluation metrics to be considered also for P1. Its validation and evaluation results will be reported for the P1 prototype.

Driven by previously defined use cases – in the 3 domains identified -, and framework architecture with the already implemented and integrated components, will stimulate validation scenarios. The main result is the acknowledge of the ARCADIAN-IoT framework and Use Cases, its components, and interrelations with each specific Domain artefacts.

With the architecture framework implementation and integration evolution validation and evaluation results will contribute to the evolution of the framework implementation. Also Use Case validation will be used as feedback enabling an ecosystem more reliable and robust.

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 research and implementation of each ARCADIAN-IoT component (addressed in WP3 and WP4), the integration of the ARCADIAN-IoT Framework (addressed in T5.1), and the preparation and implementation of the use cases (Tasks 5.2, 5.3 and 5.4). All technical partners were involved in the iterative process of integrating ARCADIAN-IoT framework.

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
BLE	Bluetooth Low Energy
CoT	Chain of Trust
CTI	Cyber Threat Intelligence
DB	Database
DID	Decentralized Identifiers
DLT	Distributed Ledger Technologies
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
FE	Functional Encryption
FL	Federated Learning
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
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
NBIoT	Narrowband Internet of Things
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
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 and related outcome (Prototype 1 - P1). It is followed by a presentation of key background information that relates to P1 (i.e., domains, use cases validation and KPI evaluation). Finally, this 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 and evaluation for the first prototype (P1)** of ARCADIAN-IoT framework. P1 provides preliminary ARCADIAN-IoT functionalities and associated integrated components, which are documented in Deliverable D5.1 (Integration of ARCADIAN-IoT framework) [1].

P1 validation depends on the availability of the use cases artifacts (e.g., service-specific software or hardware) which are being produced or adapted by the use case owners (associated to Task 5.2, Task 5.3 and Task 5.4).

P1 evaluation will follow the KPIs defined in WP3 and WP4 that will be applicable in the context of the functionalities and Use-Cases available for P1 and additional KPIs from the framework as a whole (not covered by WP3 and WP4).

P1 already considers a set of functionalities that can be validated and evaluated in the context the project's domains and respective use cases (defined in Task 5.1, 5.2, 5.3 and 5.4), and paves the way for training activities targeted for the most relevant stakeholders (Task 5.6).

1.2 Background

This deliverable builds upon several different inputs, across WP3, WP4 and WP5 (tasks T5.1, T5.2, T5.3 and T5.4). From WP3 it was used the Horizontal Components identified and specified, and the associated KPIs to be applicable for evaluation. From WP4 it was used the Vertical Components identified and specified and the associated KPIs to be applicable for evaluation. From WP5 T5.1 it was taken into consideration the integration results included in deliverable D5.1 and the Components/Use Cases availability for P1 identified during the Integration phase and the impact in the Component's KPIs to be available for P1. From WP5 T5.2 to T5.4 it was applied the Use Cases Specifications included in deliverable D5.3 taken into consideration the subset of interactions available for P1, that will conduct on the definition of the scenarios for validation and evaluation.

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 first version of the ARCADIAN-IoT framework (P1) – which directly affected the final scenarios expectable only in time for the final version (P2). The associated effort took place within the validation task (T5.5) and has involved all consortium partners, i.e., technical partners, domain owners and legal experts.

1.3 Document Structure

The remainder of this document is presented as follows:

Section 2 refer the methodology used for the validation and evaluation activities that are being applied during the T5.5 task. It details also the architectural environment used for the validation and evaluation activities, including all the integrated Framework Components (Horizontal and Vertical) and the set of Domain artefacts needed for the Use-Case-derived scenarios instantiated. It also defines the subset of Components and Use-Cases by Domain that are addressed for the current P1 validation. Finally, it details the Legal Compliance Scope addressed during P1 validation activity.

Section 3 is responsible for the description of the specification of the Validation scenarios implemented and executed during the Task T5.5 Validation. The scenario description includes for each Domain the Use-Cases validated, the involved ARCADIAN-IoT components and the scenarios implemented.

Section 4 describes for each KPI group the evaluation scenarios implemented and the measure criteria addressed for each KPI used for the evaluation.

Section 5 is responsible for the specification of the Legal compliance validation activity addressed for the P1 Prototype.

Section 6 reports the validation and evaluation results that were achieved during Task T5.5 validation and evaluation activity including both technical and legal validation for all 3 Domains, and the respective Use-Cases and Framework available during P1.

Section 7 analyses the current achievements with respect to the overall ARCADIAN-IoT project objectives and KPIs.

Section 8 summarizes the main points and achievements of the Task T5.5 and elaborate what will be expected for the second validation activity (P2).

2 METHODOLOGY, APPROACH AND SCOPE

2.1 Methodology

Given that in this intermediate P1 validation activity only a subset of the Use Cases will be completed the Use Cases selected for the validation scenarios in some cases may not be End-to-End complete scenarios, but only partial Use Cases implementations. These Use Case subsets will be listed in the Validation Scope described in section 2.3.1.

For the technical evaluation activities, it considers the metrics, KPIs specified in the present scope of the evaluation methodology (section 2.3.2), and the tools to gather the values in the diverse Use Cases. The KPIs to be considered for evaluation comprise both the framework-wide KPIs (referred in D2.5 [2] section 2.1), and the Component-specific KPIs (listed in D3.1 [3] for (Horizontal components) and D4.1 [4] for Vertical components).

The legal compliance evaluation will mainly focus on the protection of personal data processed in each Domain, taking into account, *inter alia*, the principles set forth in article. 5 of the GDPR1.

---

1 *1. Personal data shall be:*

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

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').>>

2.2 ARCADIAN-IoT Validation approach

In Figure 1 it is represented the overall validation approach that will be used during Task T5.5 validation execution. The approach comprises 2 main areas of responsibility (environments):

- Domain Specific environment: for each of the 3 Domains (A, B and C) it has to be instantiated all the needed artefacts that has to be used to participate in the specific Use-Cases that will be evaluated; each domain environment will be instantiated by each Domain respective implementation Task (T5.2 to T5.4 respectively);
- Framework environment: all the Horizontal and Vertical components will be deployed and integrated into ARCADIAN-IoT Framework during Task T5.1 execution and will be Task T5.1 responsibility to have the Framework available for the validation activities in Task T5.5.

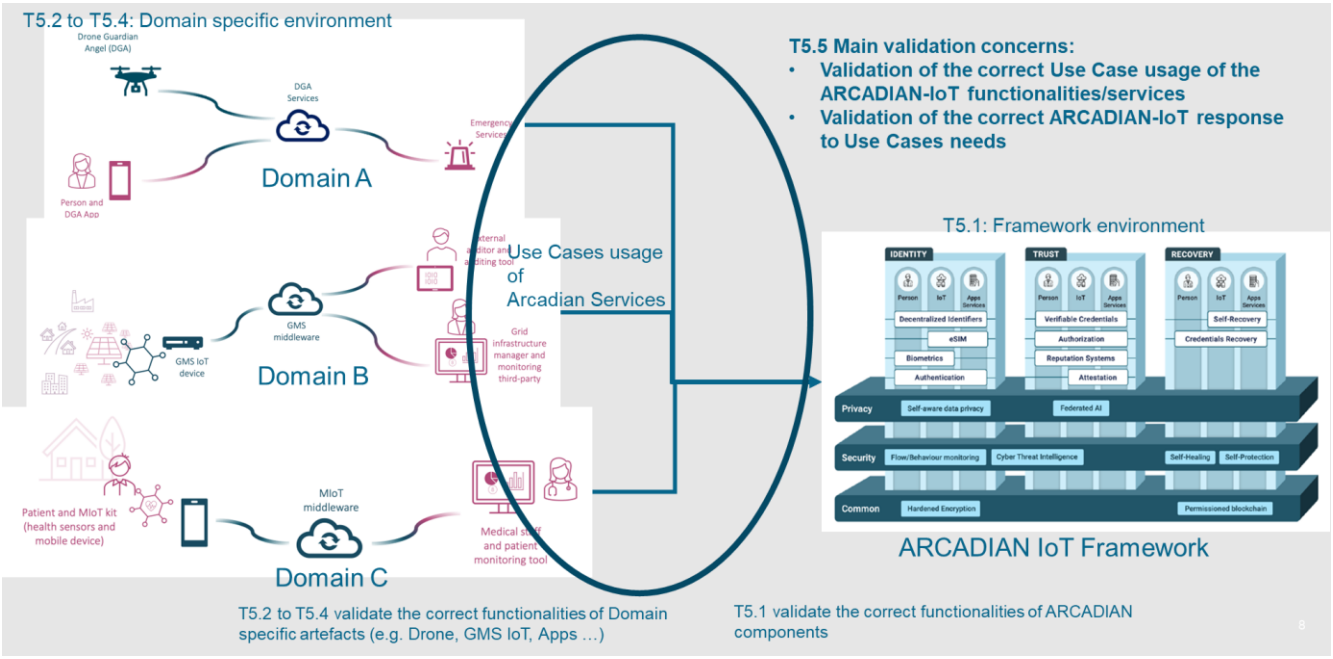

Figure 1 - ARCADIAN-IoT validation approach

Task T5.5 is responsible for the validation for each Domain, of each Use Case correct usage of the ARCADIAN-IoT components, considering both the correct usage of the Domain artefacts of the available ARCADIAN functionalities and the correspondent correct response of the Framework to the Use Case needs.

2.3 Target Scope

In the context of P1 prototype, this Deliverable will enumerate all the Use Cases and dependent components that will be available for the validation activity, and that are defined in detail by T5.2 to T5.4 in Deliverable D5.3. This Validation scope will be a subset of the complete (P2) validation that will include all Use Cases and components. In order for a Use Case / Component interaction

to be validated according to Figure 1, the Use Cases and the Components has to be ready for P1 validation. This combination of Use Cases + Components availability was defined during T5.1 (Integration Task).

For Evaluation it will be used a sub-set of the KPIs defined during WP3 and WP4, that were applicable in the scope of P1 Use Cases and were identified to have evaluation in the context of WP5 (other Use Cases will only be addressed for evaluation during internal WP3, WP4 or WP6 execution). In this context it is included either KPIs identified in the context of vertical components and KPIs identified in the context of horizontal components.

2.3.1 Validation scope

Figure 2 indicates the Use Cases (by domain) that were identified during Integration for the P1 intermediate step (included in deliverable D5.1). Depending on the degree of completion reached during integration, these Use Cases are the ones that were identified to be included for validation (e.g., “In Scope for validation” are targeted for validation; some functions in the Use Cases with the status “Partially Used for Validation” status will be selected also). The remaining use cases are targeted for P2 validation.

P1	In scope for validation
P1	Partially used for validation
P1	Not in scope for validation
P2	Planned for P2
	Not involved

				Use Cases							
				A1	A2	A3	B1	B2	C2	C3	C4
				Person registration at DGA service	Person authentication at the DGA service	Person retrieving and editing personal data	New device registration	GMS IoT device data gathering and transmission process	MIoT Capturing and sending vital signs and perceived health status	Personal data processing towards health alarm triggering	Monitor a patient and update a patient monitoring protocol
				LOAD	LOAD	LOAD	BOX2M	BOX2M	RGB	RGB	RGB
				P1	P1	P1	P1	P1	P1	P1	P1
Vertical plane	*Identity*	Decentralized identifiers	ATOS	P1	P1		P2	P2	P1		P1
		Network-based authentication of IoT devices in third-par	TRU	P2	P1						
		Biometrics	UWS	P1	P1	P2					
		Multi-factor Authentication	TRU	P2	P1			P2?			
	Trust	Verifiable credentials	ATOS	P1	P1				P1		P1
		Network-based authorization enforcement	TRU	P2	P2	P2	P2	P2	P2	P2	P2
		Reputation Systems	UC	P1	P1	P1	P2	P2	P2	P2	P2
		Remote Attestation	IPN			P1	P2	P2	P1		
	Recovery	Self-recovery	XLAB				P2				
		Credentials Recovery	ATOS				P2				
Horizontal plane	*Privacy*	Self-aware data privacy	MAR	P2		P2	P2	P2	P1	P1	P2
		Federated AI	RISE								
	Security	Behaviour Monitoring	IPN	P2	P2	P2	P1	P1	P2	P2	P2
		Network Flow Monitoring	UWS								
		Cyber Threat Intelligence	RISE								
		Network Self-Healing	UWS								
		Network Self-Protection	UWS								
		IoT device self-protection	IPN								
	Common	Hardened Encryption (via eSIM)	XLAB	P2	P2	P2			P1	P1	P2
		Hardened Encryption (via cryptochip)	BOX2M				P1	P1			
		Permissioned blockchain	ATOS	P1	P1	P1	P2	P2	P1		P1

Figure 2 - P1 Use Cases and applicable components

In Figure 2 the states applied for the 8 **Use Cases** (upper right section) have the following meaning:

- "In Scope for Validation": the Use Case is P1 and is considered for validation.
- "Partially used for Validation": the Use Case is P1 available but is only partially considered for validation (only some functionalities).
- "Not in Scope for Validation": the Use Case, even being considered as P1, it was not ready for validation during P1.

At the same time, Figure 2 also depicts the states applied for the 21 **Components** (lower left section). The states have the following meaning:

- "In Scope for Validation": the Component is P1 available in the context of the Use Case and is considered for validation.
- "Partially used for Validation": the Component is P1 available in the context of the Use Case but is only partially considered for validation (only a sub-set of interactions).
- "Not in Scope for Validation": the Component even it was considered as P1 available in the context of the Use Case it was not ready for validation during P1.
- "Planned for P2": Components that will be used in the context of the Use Case but only ready for validation during P2.
- "Not involved": Component that does not participate in the Use Case execution, so will not be validated.

The table depicted in Figure 2 has some differences with respect to the Integration Table previously presented in D5.1. This is a natural result from the performed work (e.g., increased clarity / maturity of the validation targets) and associated decisions. The differences are the following:

- The **Self-aware Data Privacy** component will no longer be involved in A1 and A3. Moreover, the involvement with B1 and B2 are postponed to P2.
- The **Remote Attestation** will no longer be involved in A1; the corresponding interactions are instead a pre-condition for performing remote attestation procedures (e.g., A3).
- **Multi-factor authentication** has been already validated in A2 in the scope of P1
- **Hardened Encryption (via eSIM)** will only be validated in C3 the scope of P2.
- **Blockchain** with the Publisher smart contract was tested to publish data sets during April and is now in active integration phase with Hardened Encryption & Reputation components. Additionally, the blockchain was integrated with the Decentralized Identifier component, based on the DIF Sidetree specification[2] for providing the trust in the public Decentralized Identifiers.

2.3.2 Evaluation scope

The KPIs for evaluation of ARCADIAN-IoT components were defined in WP3 (for Horizontal planes' components) and WP4 (for Vertical planes' components). It was specified that, from the whole list of KPIs, some are able to be evaluated as part of horizontal / vertical plane research activities (i.e., WP3 or WP4, and reported under associated deliverables) while others are evaluated as part of (ARCADIAN-IoT or domain) integration activities.

This deliverable addresses only KPIs evaluated in the context of WP5. Finally, from these KPIs,

[2] https://identity.foundation/sidetree/spec/

only KPIs from those components that are involved and already available in P1 use cases (identified in Figure 2 of the previous section) are scoped for evaluation.

In the context of P1 Evaluation it was not defined other KPIs (e.g., Arcadian transversal KPIs or Arcadian Framework KPIs) than the ones that came from the Component KPIs identified. The possibility to add additional KPIs will be considered during P2 Evaluation Phase.

The detailed list and explanation of the included KPIs and how to measure them are addressed in section 4.

2.3.3 Legal compliance scope

As depicted in previous deliverables (e.g., D2.1 and D2.3), ARCADIAN-IoT technology potentially raises legal compliance risks related to the adoption of IoT, drones and facial recognition mechanisms.
Therefore, the legal compliance evaluation will focus on those technologies, which and how the data will be exchanged among them, in order to ensure that the citizens can exercise their rights in terms of personal data protection (anonymised or pseudonymised data), control over data and data accuracy, transparency of technology (especially for what concern the facial recognition mechanisms), proportionality of data collection (especially for drones).
All those technologies will be therefore analysed in the light of the current relevant European legal framework, including, *inter alia*, the General Data Protection Regulation.

3 VALIDATION SPECIFICATION

3.1 Introduction

In this section it is described the Validation Specification that was planned to be executed during T5.5 validation activity. The specifications have, as main input, the Use-Cases defined in-scope for P1, enumerated in 2.3.1. These Use-Cases are detailed in Deliverable D5.3 and summarized in these subsections using Sequence Diagrams elaborated in collaboration with T5.2, T5.3 and T5.4.

Using the selected Use Cases and taking into consideration only P1-ready Use Cases and Components listed in Figure 2, one (or more if needed) validation scenario(s) were defined for each use case. These Validation Scenarios detail the specific flows and information data used for the validation of each Use Case.

3.2 Domain A - Emergency and Vigilance

All Domain A Use Cases are described in detail in Deliverable D5.3 (Section 3). This section summarizes the Use Cases that are ready for P1. Moreover, only the subset of interactions with the components that are ready for P1 validation are considered (also depicted in Figure 2).

3.2.1 Use-Case A1 - *Person Registration at DGA Service*

Prerequisite conditions:

- Obtain a mobile with a camera and an eSIM provided by Truphone.
- Download, install the DGA App on mobile & configure Fingerprint access.

These following actions are required for the validation of Prototype 1:

1. Open DGA App & click on links to Registration & sub-link to be issued with user mobile wallet identity to the user´s SSI Wallet.
    a. Download, Install the SSI Wallet App on mobile & configure Fingerprint access.
    b. Click on link to be issued with a mobile wallet identity, and user resultantly receives an identity in their wallet.
2. Now that the user has a wallet identity, he/she 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 which shows a QR Code and link (to click on if seen on a mobile) to present their mobile wallet identity.
    NOTE: The user is informed to open their mobile wallet before proceeding to click on the link.
    b. The user clicks on link and receives a request on mobile to present their Person Verifiable Credential that was previously issued to them.
    c. The user confirms the presentation.
3. 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.
4. User is asked to provide photo images to finish the registration and the user provides their

images as requested by the app.
5. User is informed on the DGA app that their registration is complete.
6. Registration event is sent to the ARCADIAN-IoT Framework with Person Identity and new aiotID.
7. ARCADIAN-IoT Framework services in P1 (Reputation, Self-Recovery) initialise their respective services for the new aiotID.

3.2.2 Use-Case A2 - *Person authentication at the DGA service*

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 validation scenario is the following:

1. The person has a smartphone with the DGA app installed, the SSI Wallet (Ledger uSelf android wallet app), and communicates using cellular networks (e.g., LTE or 5G) with a TRU eSIM/SIM.
2. Using the DGA app to authenticate, the person will be requested to take a photo. The app will send, in a secure way, to its (DGA) backend, this photo appended to the ARCADIAN-IoT ID it wants to authenticate.
3. Communicating through the cellular networks, when the request passes through the core network infrastructure, an ARCADIAN-IoT component (*Notarizer*) appends to the authentication request a signed and protected Network ID token (transparent to the user).
4. The person authentication request follows to the DGA backend services, which, for using ARCADIAN-IoT MFA services, forwards the request to the MFA component.
5. The MFA splits the request received, asking: (1) ARCADIAN-IoT's Biometrics component to confirm if 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.
6. 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.
7. The SSI component will establish 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.
8. If the three authentication factors verification is 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, which returns it to the requesting personal device – the person is now authenticated and can proceed with the use of the DGA mobile app.
9. 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.

Functionally the expected result from the scenario above is to have a person authenticated using the three authentication factors.

The technical and detailed sequence diagram correspondent to the scenario above is shared among the involved partners in the project online folder.

3.2.3 Use-Case A3 - *Person retrieving and editing personal data*

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 authenticate, as per the A2 use case.

The following actions are required for validating the use case:

1. Using the DGA App, the person supplies some personal data to the DGA service, which includes name, address, photo, and optional SOS contacts.
2. The DGA service, before providing the requested data to the user, requires reputation information from the user and its personal device.
3. Upon the reputable 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. If 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.

The expected results of A3 include:

1. Encryption of data, in the device and on the communication channel between the DGA app and the DGA service.
2. Employment of reputation values provided by the reputation system to authorize the personal device to access to the network, and consequently to exchange data with the

DGA service.

3. Successful attestation of smartphone device according to IoT service provider policies (dummy data matches the “acceptable” device integrity status)

3.3 Domain B - Grid Infrastructure Monitoring

In this section it will be summarized the Use-Cases that have P1 readiness. It is also be taken into consideration only the subset of interactions with the components that are ready for P1 also (see Figure 2.). Domain B Use-Cases associated to P1 are described in detail in Deliverable D5.3.

3.3.1 Use-Case B1 – New Device Registration

Several actions are required to validate this use case. The execution success (or failure) of the associated actions - part of the technical validation process described next - will be registered and analysed in section 6.2. The following components are involved in the validation scenario planned for P1: **Device Behaviour Monitoring** and **Hardened Encryption (via Crypto chip)**. Therefore, this use case’s validation actions also consider the correct integration and interfacing with the beforementioned components.

The remaining components that are involved in use case B1, as described in document D5.3, Section 4.2, are a target of Prototype 2. Therefore, their integration and interfacing validation will take place on the second round of validation activities, due on M30.

These are the actions considered for validation:

1. Turn on an unregistered device with compiled firmware previously loaded.
2. Connect with O&M set-up kit on device and from device firmware configuration CLI (Command Line Interface), by local logging to device with BOX2M provided user and password, and using a local encryption method (“OTS – over the serial”):
   2.1. Install eSIM or SIM profile (APN name, user, password), depending on chosen SIM type; during authentication, these data correlated with SIM / eSIM IMSI and / or modem IMEI, can be used by Truphone Authentication System or other operator Authentication System to decide if Device is able or not to authenticate and perform data traffic.
   2.2. Set-up the communication module type (GSM, UMTS, LTE, LTE-M, NBIoT, 5G, ETH, WiFi, ETH & WiFi).
   2.3. Set-up the communication failover option (if the device is equipped accordingly, with specific communication extension board).
   2.4. Set-up Device ID, user and password
   2.5. Set-up Middleware contact point (telemetry broker address - domain name, port number)
   2.6. Call encryption keys generation function, defined into crypto chip library by crypto chip vendor (Infineon), which is part of device firmware libraries, to randomly generate keys for authentication, traffic and recovery stages.
   2.7. Take note of the keys (optimally not on electronic devices, to do not leave traces which may be a vulnerability point), to be defined into Middleware side too; destroy the notes after Middleware definition; make sure the randomly generated keys are unique (by

comparing with keys from previously registered devices)[3];

2.8. Activate the log monitor on a terminal application of O&M laptop, keeping device connected.

3. Connect to Middleware frontend address and login by user & password provisioned previously by BOX2M and by code generated with a multi factor authentication service integrated into Middleware (provided by Microsoft).
   3.1. Into “Devices” menu, “General” sub-menu, define new device, with the ID, user and password used in 2.5., check mark the options “Show in reports” and “Is enabled”.
   3.2. In “Devices” menu, “Encryption” sub-menu, define “Use Key 1” with the value generated at 2.7. for authentication, “Use Key 2” with the value generated at 2.7. for traffic, “Use Key 3” with the value generated at 2.7. for recovery.
   3.3. Set-up the Behaviour Monitoring function (which was hardcoded into Middleware, not by GUI/front end), for both Docker containing the Middleware and for the new provisioned device. Every time a new device is added into the fleet, it must be defined into behaviour monitoring too. Every time an existing device is removed from the fleet, it must be erased from behaviour monitoring too.
   3.4. Set-up the connection with Message Bus of the ARCADIAN-IoT Framework (in order to send messages to the Behaviour Monitoring System)
   3.5. Publish device ID (i.e., ARCADIAN-IoT ID) to Device Behaviour Monitoring (DBM) and to the Reputation System via the dedicated exchanges/queues.
   3.6. Configure the relaying of devices’ authentication events to the Device Behaviour Monitoring (DBM)
   3.7. Configure the periodic push (i.e., every 30 seconds) of aggregated system calls (associated to the Middleware’s container) to Device Behaviour Monitoring (DBM).
   3.8. Configure (hardcoded) the Middleware API to IoT platform chosen to manage the sensors and devices data; reason is to perform a relay translation between each decrypted message received from device and forward TLS encryption for communicating the message with IoT platform
4. Reset the device and monitor:
   4.1. On terminal application of O&M laptop, the settings done between 2.1. to 2.7. to be kept as defined
   4.2. On terminal application of O&M laptop, the success or failure state of device connection to network operator data services and to Middleware telemetry broker; if the network operator will deny the connectivity, or any of the encryption keys, Device ID, Device user or Device password do not match with provisioned data, these will be showed explicitly in terminal logger (supported by firmware designed for this local debugging / monitoring); obviously, showed data is not in clear, being output just the encrypted string
   4.3. On Middleware SOC (service operation centre), into “Devices” menu, “MQTT messages” sub-menu, either “MQTT Messages” option (for real time, processed messages), or “MQTT messages raw” option (for real time, not processed messages), the success or failure state of device connection to Middleware telemetry broker and into IoT platform; if encryption keys, Device ID, Device user or Device password do not match with provisioned data, these will be showed explicitly into message in this sub-menu option
   4.4. Forward messages to the Behaviour Monitoring System to enable monitoring and perform

[3] This redundancy check operation can be done from Middleware, hardcoded option for time saving reasons (else the operator should take device by device and compare the keys).

post reporting (per certain criteria) of associated events.

According to the integration plan, **use case B1 has been finalized and successfully integrated** with a set of ARCADIAN-IoT components, being ready for validation within P1 (validation results described in the following sections). The remaining components are to be integrated and validated for P2.

3.3.2 Use-Case B2 - GMS IoT device data gathering and transmission process

These are the actions considered for validation:

1. Turn on an unregistered device with compiled firmware previously loaded.
2. Connect with O&M set-up kit on device and from device firmware configuration CLI (Command Line Interface), by local logging to device with BOX2M provided user and password, and using a local encryption method (“OTS – over the serial”):
   2.1. Set-up the circuits (representing a physical or virtual sensor) ID's.
   2.2. Set-up for each circuit, parameters ID's (parameters are representing measurements or message types returned by physical or virtual sensors, during lifecycle operations, according to sensor vendor definitions).
   2.3. Set-up for each parameter the frequency sampling rate of transmission to IoT platform empowered to manage the data.
   2.4. Activate the log monitor on a terminal application of O&M laptop, keeping device connected.
3. Connect to Middleware frontend address and login by user & password provisioned previously by BOX2M and by code generated by a multi factor authentication service integrated into Middleware (provided by Microsoft).
   3.1. Into “Devices” menu, “Circuits” sub-menu, define new circuits, one by one, for each with their IDs and parameter IDs (these belonging to a type and name of sensor, and with a customized set of data processing rules, if applicable, sensor type depending) used into 2.2.; set-up the circuit to be “Show in reports”.
4. Connect the device to sensors kit, power up sensors, reset the device and monitor:
   4.1. On terminal application of O&M laptop, the settings done between 2.1. to 2.3. to be kept as defined.
   4.2. On terminal application of O&M laptop, the network operator authentication success and data bear allocation, the Middleware telemetry broker encrypted authentication success or failure and then the success or failure of encrypted – with key 3 / traffic type - payload transmission of the previously defined circuits and parameters, on the previously defined frequency rate.
   4.3. Anytime device reboots / restarts, the whole encryption process is retaken from scratch (including authentication); else, if device stays powered, and network operator infrastructure maintains the data connection, and Middleware closes a traffic session, than when another traffic session is started by device, another encryption session for traffic will be started (using again Key 3 as reference for crypto chip to perform the payload encryption); these will be showed explicitly into terminal logger, firmware being designed for this local debugging / monitoring purpose too; obviously, showed data is not in clear, being output just the encrypted string.
   4.4. On Middleware SOC (service operation centre), into “Devices” menu, “MQTT messages” sub-menu, either “MQTT Messages” option (for real time, processed messages), or “MQTT messages raw” option (for real time, not processed messages), the success or failure state of device traffic transmission to Middleware telemetry broker; if encryption

key do not match with provisioned data, these will be showed explicitly into message in this sub-menu option.

4.5. Forward messages to the Behaviour Monitoring System to enable monitoring and perform post reporting (per certain criteria) of associated events.

According to the integration plan, **use case B2 has been finalized and successfully integrated** with a set of ARCADIAN-IoT components, being ready for validation within P1 (validation results described in the following sections). The remaining components are to be integrated and validated for P2.

3.4 Domain C - Medical IoT

All Domain C Use-Cases are described in detail in Deliverable D5.3 Section 5. In this section it will be summarized the Use-Cases that have P1 readiness. It is also be taken into consideration only the subset of interactions with the components that are ready for P1 also (see Figure 2).

3.4.1 Use-Case C2 - MIoT capturing and sending vital signs and perceived health status

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 below (Use case C3).

Within the purpose of P1 validation, the following Arcadian-IoT components have been deployed and tested in this use case C2: Hardened Encryption, Self-Aware Data Privacy (SADP) and Remote Attestation.

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

<u>The following pre-conditions need to be validated due to the dependency that other use cases have on them: the attester is running in background on the device (Smartphone).</u>

a) The devices successfully received 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 uses attribute/public key to decrypt data.
d) Proxy service receives policies from the Telemed service.
e) Proxy encrypts data with received policies
f) The Telemed Service received encrypted data and stores it.
g) Telemedicine Service, Self-Aware Data Privacy, Hardened Encryption Libraries are deployed in the same secured environment e.g., physical machine.

<u>The following actions are required for validating the use case:</u>

1. The device collects patient vital signs captured by the medical sensors.
2. 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.
3. The HTTP request containing the data is intercepted by the SADP component
4. The SADP component retrieves the encryption polices from the Telemedicine Web Service
5. The SADP component leverages sends and encryption request to the HE library with the retrieved policies.
6. The HE library encrypts the data according to the retrieved policies and returns them to the SADP.
7. The SADP component sends the encrypted data to the telemedicine web service for their secure storage in the telemedicine database.
8. 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.

3.4.2 Use-Case C3 - Personal data processing towards health alarm triggering

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. While Self-aware data privacy, Hardened Encryption (HE), Reputation system, and Network-based authorization enforcement components are used in this use case, only the first two are validated in the P1.

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

3.4.3 Use-Case C4 - Monitor a patient and update a patient monitoring protocol

Prerequisite conditions:

a) Patient is previously registered in the MIoT mobile app as per Use case C1.
b) Medical Professional is registered in the MIoT Hospital platform which is integrated with

the ARCADIAN-IoT framework – as this prerequisite was only defined at a later stage of the requirements, this prerequisite will only be fulfilled at a later stage due to the ongoing technical development to support the scenario.

The following actions are required for the validation of Prototype 1:

1. A medical professional access the MIoT hospital platform and chooses to be authenticated by ARCADIAN-IoT Framework (based on network eSIM token and SSI)
2. The medical professional is requested to open their mobile wallet before confirming to proceed to request their Organisation Verifiable Credential from the mobile wallet.
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.
    a. As part of this process the reputation of the medical professional is checked, and a low reputation could be a reason to deny access.
4. The medical professional accesses their patients´ dashboard to view any alerts or a specific patient´s data. The data that it receives comes from Use Cases C2 and C3 but in unencrypted form since integration with Hardened encryption and Self-aware data privacy is scheduled for P2.
5. Real-time requests for data can be made to the patient´s mobile app, such as a request to change the monitoring protocol. Authorization of of these requests and encrypting the communicated data is scheduled for P2.
6. Medical professional login should be captured in MIoT hospital platform or SIEM.
7. The medical professional should be able to view patient data retrieved in real-time.
8. The patient should be 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.
9. When the reputation of the medical professional is reduced then it can be seen that an event is raised in the MIoT hospital platform and that the medical professional is denied access to the platform.

4 EVALUATION SPECIFICATION

4.1 Introduction

This section describes the Evaluation Specification that was planned to be executed during T5.5 evaluation activity. The specifications have, as main input, the KPIs defined in the scope of P1. These KPIs are detailed in Deliverables D3.2 and D4.2, and summarized in section 2.3.2.

Using the selected KPIs, and taking into consideration only the P1 readiness (Use-Cases and Components), listed in Figure 2, it was defined one (or more) evaluation scenario(s) for the measurement of each KPI. These Evaluation Scenarios details the flows and information data used for the evaluation of each KPI.

4.2 KPIs Associated to Components Evaluated in P1

The KPIs that were included for evaluation during P1, which scope is explained in section 2.3.2 are summarized below (including the information in the format *[Component Name] TargetValue)*:

1. **Horizontal component's dependant KPIs**

- [Permissioned blockchain] Number of ARCADIAN-IoT services using permissioned blockchain = 3
- [Permissioned blockchain] Number of peer nodes deployed = 3
- [Behaviour monitoring] Number of inputs considered >= 3 sources of information of IDS
- [Behaviour monitoring] Number (Type) of supported devices >= 2
- [Hardened Encryption (with eSIM)] Number of languages and platforms supporting HE => Provide encryption library enabling fine-grained access control over data with APIs in at least 4 programming languages and demonstrate its use on at least 2 types of devices/platforms.
- [Hardened Encryption (with eSIM)] Timing of encryption/decryption with HE (low overhead) => Efficient implementation with encryption times comparable to the state-of-the-art results on multiple devices.
- [Hardened Encryption (with crypto chip)] Provisioning time (for any scenario) into device side and middleware side, via a CLI or web GUI => feasible and rapid implementation of technology for system integrators / other skilled operators compared with existing SCADA / BMS configuration fulfilment environments, defining state-of-the-art for this industry
- [Hardened Encryption (with crypto chip)] Timing of encryption for communication segment between IoT device and middleware, and for segment between middleware and IoT platform managing the sensors data => Efficient implementation with encryption times facilitating real- & feasible-time grid infrastructures monitoring

2. **Vertical component's dependant KPIs**

- [Decentralized Identifiers] Support at least two of the use case domains >=2
- [Decentralized Identifiers] Support authentication for persons and IoT devices
- [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 (Y/N)
    - Number of different devices where the innovation is demonstrated >=2
    - TRL >=6
- [Biometrics] Low Inference Time for Face Verification Algorithm <= 16 FPS
- [Biometrics] High Accuracy of the Face Verification Algorithm (<2m)[4] <= 90%
- [Biometrics] Reliable Recognition of the Face Verification Algorithm <= 0.5% FAR
- [Multi-factor Authentication] Novel multifactor authentication component joining hardware-based identification with decentralized identification and biometrics
    - Number of simultaneous different identification factors for persons: 3
    - Number of simultaneous different identification factors for devices: 2
    - Number of devices used simultaneously in a person's identification: 2
- [Verifiable Credentials] Issue person Verifiable credential with an eIDAS compatible schema => Support interop with one eIDAS schema
- [Remote Attestation] Number of devices/OS platforms supported by remote attestation >=2
- [Remote Attestation] Types of IoT devices reputation affected by RA >=1
- [Remote Attestation] Number of IoT services reputation affected by RA >=1
- [Reputation System] The associated KPIs include:
    - Types of entities supported (persons, devices, services) >= 3
    - Time to process an event < 1second
    - Number of messages analysed by time unit: 10 per second

4.3 Measurement Plan for KPIs

This section describes the detailed information regarding how the KPIs were measured, by using scenarios addressed for evaluation. The measurement of the component-dependant KPIs will be described in each Component dedicated section.

4.3.1 Permissioned blockchain KPIs

Permissioned Blockchain will support Decentralized Identifiers and publishing Hardened Encryption public keys in the P1 validation.

- **Number of ARCADIAN-IoT services using permissioned blockchain in P1 = 2**
    - ARCADIAN-IoT SSI Agent using Sidetree based Decentralized Identifier (DID:ELEM) in P1 with trust rooted on private Ethereum blockchain
    - Hardened Encryption publishing public key material on Hyperledger Fabric in P1 for the associated aiotID.

- **Number of peer nodes deployed = 3**
    - Hyperledger Fabric deployed in 3 nodes on pre-production VM hosted by ATOS

4 The KPIs >2m will be only considered during P2, using Use-Cases A4 and A5

for P1.

- Private Ethereum deployed in 3 nodes on pre-production VM hosted by ATOS for P1.

4.3.2 Behaviour Monitoring KPIs

The Device Behaviour Monitoring (DBM) component will be validated in several use cases in all three domains. The complete validation is split between P1 and P2 prototypes. In the scope of P1 (reflected in this deliverable) this component will be validated on Domain B and its use cases B1 and B2, respectively. The complete set of KPIs and validation in the remaining use cases will be part of P2 validation activities.

- **Number of inputs considered >= 3 sources of information of IDS**

  This KPI intends to measure the number of inputs that the Device Behaviour Monitoring component can process (i.e., information considered during the intrusion detection classification). The development roadmap of this component until the final Prototype of the ARCADIAN-IoT Framework (P2) considers the processing of the following inputs:

  - **System Calls**

    System Calls are a programmatic way in which a computer program (i.e., a process) requests a service from the kernel of the operating system it is executed on. The DBM analyses patterns of system calls and triggers alerts when anomalous patterns are identified.

  - **Authentication Events**

    Authentication events are the information associated to the authentication on the device (or service - when applicable) in question. The number of unsuccessful attempts and the time window between each attempt are the main factors to be considered by the DBM.

  - **Reputation Events**

    Reputation Events are provided by ARCADIAN-IoT's Reputation System. The reputation system ingests events from several ARCADIAN-IoT components. Thus, the reputation of the device is updated according to various factors (e.g., failed authentication attempts, device loss, security incident or privacy incident). The main factors the DBM considers with respect to reputation are (1) the current reputation of the device and (2) the delta (i.e., the differential) of each reputation change.

  P1 validation considers the following input, in different use cases:

  a. Authentication Events
     i. Use case B1
     ii. Use case B2

  The remaining inputs that are part of this KPI will be fully verified upon delivery of Prototype 2 and the deployment of the DBM in P2 use cases. With respect to system calls, the access and collection of system calls has been proved possible by being able to run the

device behaviour monitoring and extracting the relevant system calls. Up to now, it was possible to (1) perform this action directly on the Drone Hardware, supported by a Jetson Board (part of Domain A and P2), as well as (2) capturing system calls from a running container deployed by Docker or Kubernetes.

- **Number (Type) of supported devices >= 2**

  This KPI intends to measure the number of different devices where the Device Behaviour Monitoring component can be deployed and directly executed. The support for device heterogeneity can be explicitly measured with one of the following metrics:

  - **Number of Supported Operating Systems**

    The DBM component is expected to support execution on at least 2 different operating systems (e.g., Linux or Android). The validation of this KPIs will assess the proper execution of the component on Linux-based devices, as well as IoT Gateways such as a smartphone (present in Domain A and Domain C).

  - **Device Category**

    Similarly, this KPI may also be assessed by the ability to deploy in different kinds of IoT devices (e.g., drones, IoT gateways or devices for sensor data aggregation). As such, in the context of ARCADIAN-IoT and its validation domains and scenarios, Domain A considers drones and IoT Gateways such as smartphones with Android operating system, Domain B considers devices specialized in IoT sensor data aggregation and Domain C considers specialized IoT Gateways (i.e., smartphones) that interface with Medical IoT Kits (e.g., hearth rate sensors or blood pressure sensors).

    Due to hardware constraints, the device behaviour monitoring deployment is applicable to Domain A and C devices only. For the monitoring of domain B devices and sensors to be possible, BOX2M's custom-made IoT device and middleware will relay tailored activity events to a dedicated DBM instance deployed elsewhere.

  P1 validation considers the following device types:

  a. Linux-based devices
     i. Use case B1
     ii. Use case B2

  Even though the current validation scenarios and use cases do not target other device categories and operating systems, ongoing work has already shown preliminary support for drones based on NVIDIA's Jetson Hardware (part of Domain A). As such, in the scope of P2 validation, the DBM will be deployed directly on drones, as well as on Android devices (part of Domain A and Domain C).

4.3.3 Hardened Encryption KPI

The Hardened Encryption (HE) component consist of two subcomponents namely Hardened Encryption with eSIM as RoT and Hardened Encryption with Crypto chip as RoT.

Hardened Encryption with eSIM as RoT will be validated in several use cases in domains A and C, both in P1 and P2 prototypes. The KPIs of this subcomponent that will be evaluated in P1 are the following:

- **Provide an encryption library enabling fine-grained access control over data with APIs in at least 4 programming languages and demonstrate its use on at least 2 types of devices/platforms.**

The HE component provides an encryption/decryption library based on Attribute Based Encryption paradigm allowing fine-grained access control over the data that is encrypted. In Use case C2, the encryption library is integrated in an Android App using provided Java interface and is running on a smart phone. In Use case C3 the library with Python bindings is integrated at the server side of the MIoT service, running on a Linux server. Furthermore, ARCADIAN IoT Self-aware data privacy component integrates the Go based HE library, hence this version is (indirectly) also validated in C2 and C3, where this component participates. Finally, ARCADIAN IoT Attestation components uses Python APIs to secure data (A1, A3, C2), further validating this KPI.

- **Provide efficient implementation of the process with encryption times comparable to the state-of-the-art results on multiple devices, and with RoT signatures in acceptable time for the communication processes.**

As part of C2 and C3 we validate that the HE library encryption/decryption process is comparable to state-of-the-art values found in literature : Encryption on a laptop with 1.60GHz Intel Quad-Core i7 ~160ms for a policy with 5 attributes, Encryption on an Android phone with 1.60GHz Intel Atom Z2460 ~2.5s for a policy with 5 attributes, decryption on a laptop with 1.60GHz Intel Quad-Core i7 ~250ms for a policy with 5 attributes and decryption on an Android phone with 1.60GHz Intel Atom Z2460: ~6s for a policy with 5 attributes. RoT signatures will be validated in P2.

Hardened Encryption with crypto chip as RoT will be validated in all use cases of domain B, both in P1 and P2 prototypes. The KPIs of this subcomponent that will be evaluated in P1 are the following:

Provisioning time (for any scenario) into device side via a CLI and into middleware side, via a web GUI, to generate a feasible and rapid implementation of technology for system integrators / other skilled operators who will be the users of technology.

These times are belonging to “operation times” category, should being around minutes for a new device onboarding or an existing device modification. As benchmark, there was used legacy automation technologies, as SCADA or BMS configuration fulfilment environments.

Both target times for P1 prototype of this KPI were **achieved** for a device onboarding from scratch (which is the longest possible operation), specifically less than 5 min using CLI and less than 2 min using GUI.

Timing of encryption for communication segment between IoT device and middleware, and for segment between middleware and IoT platform managing the sensors data is significant for implementation of technology, knowing the nature of commercial applications with grid domain, where monitoring must be done in real time. They are part of “computing times” category.

T1_E – a KPI reflecting time duration between sensors data stream aggregation and encrypted

payload generation, by device firmware agent designed and build for encryption, was **achieved**, being under 2 sec. This indicator is applicable for sense device – to – IoT platform.

T2_D – a KPI reflecting 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, **was not achieved yet**, being at 12 sec and targeting 8 sec. This indicator is applicable for sense device – to – IoT platform and will be optimized during P2 development.

T4_D & T3_E KPI's are part of P2 prototype development.

4.3.4 Decentralized Identifiers KPIs

Decentralized Identifiers will support privacy preserving pairwise DIDs in the SSI Wallet and DID:ELEM for the SSI Agent in the ARCADIAN-IoT Framework in P1.

- **Support at least two of the use case domains >=2**
  - Pairwise DIDs for SSI Wallets and public DIDs for the framework´s SSI Agent are supported for use case domains A and C in P1.

- **Support authentication for persons and IoT devices**
  - Authentication attempts should be logged. Successful authentication for Persons will be captured in P1 whereas authentication of IoT Devices can be captured in P2.

4.3.5 Network-based authentication KPIs

Network-based authentication is expected to be always integrated in the Multi-Factor Authentication scheme, therefore, always assessed jointly with it.

- **Leverage cellular network authentication processes in a new zero-touch authentication of IoT devices in third-party services (Y/N)**

The network-based authentication has been validated as described in the use case A2 (section 3.2.2). The successful functional integration and testing by a IoT solution provider (as in A2) allows to evaluate this KPI as successful.

  - Number of different devices where the innovation is demonstrated >=2

In the authentication validation scenario described in the use case A2 (section 3.2.2), allows to partially demonstrate this KPI. It is expected to demonstrate it in a IoT device in the next stage (P2), to be possible to evaluate this KPI as successful.

  - TRL >=6

The EC defines TRL 6 as “technology demonstrated in relevant environment”[5]. For evaluating this KPI as successful we will consider the demonstration of the technology integrated in at least one IoT solution from one partner, e.g., ARCADIAN-IoT Drone Guardian Angel solution, in its final version by the end of the project.

4.3.6 Biometrics KPIs

The Biometrics component takes place in three use cases: A1, A2 and A3. In order to meet the requirements of the system to perform optimally with high accuracy and speed, three out of seven KPIs can be measured and evaluated using the scenarios addressed.

- **Low Inference Time for Face Verification Algorithm**

  This KPI measures the speed of the face verification algorithm and is expressed in frames per second (FPS). It can be calculated in all three use cases, A1, A2, and A3. Every time an image is received, the biometrics component logs the time taken to execute the face verification algorithm. The target value for this KPI is 16 FPS, which corresponds to 62.5 milliseconds per image.

- **High Accuracy of the Face Verification Algorithm (<2m)**

  This KPI measures the accuracy of the face recognition algorithm when the photo of a person is taken at a close distance (less than 2 meters). It is expressed in mean Average Precision (mAP) and can only be calculated over a testing dataset. This KPI is relevant for use case A2, which involves person authentication. The target value is to achieve at least 90% accuracy.

- **Reliable Recognition of the Face Verification Algorithm (<2m)**

  This KPI measures the false acceptance rate (FAR) of the biometrics component when the photo of a person is taken at a close distance (less than 2 meters). It can also be evaluated over a testing dataset, and it is qualitative measured in use case A2. The target value for this KPI is to achieve a FAR of less than 0.5% and still maintaining the high accuracy described in the previous KPI.

4.3.7 Multi-factor Authentication KPIs

The novel multifactor authentication component, joining hardware-based identification with decentralized identification and biometrics, will be evaluated integrated with IoT solution providers technologies, targeting the related ARCADIAN-IoT objectives. Follows the current validation of the defined KPIs.

- **Number of simultaneous different identification factors for persons:** 3

This KPI was targeted in P1, leveraging the 3 identification factors previously mentioned, in the use case A2 (section 3).

[5] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

- **Number of simultaneous different identification factors for devices:** 2

Following a strategic decision, this KPI will be targeted in P2. The decision to tackle first the person authentication was due to the fact that device authentication, in what concerns MFA, is expected to be just a subset of that mechanism (excluding the biometrics). This KPI is expected to be validated in the 3 domains (with 3 IoT solution providers).

- **Number of devices used simultaneously in a person's identification:** 2

This KPI is expected to be validated in P2 within Domain A, having the personal device and the drone as the 2 devices to be used simultaneously in a person's identification. Considering that it is a person authentication, the 3 different identification factors are expected to apply as well.

4.3.8 Verifiable Credentials KPIs

- **Issue person Verifiable credential with an eIDAS compatible schema => Support interop with one eIDAS 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
  - Verifiable Credential Issuer to support EBSI DID in P2

4.3.9 Remote Attestation KPIs

For P1, the Remote Attestation component will be involved in the A3 and C2 use cases. For both use cases, the RA's Verifier ability to collect reference values from IoT service providers is established as a pre-condition. In A3 and C2, the RA's Attester basic functionalities and remote attestation procedure will be validated (with dummy claims data).

- **Number of devices/OS platforms supported by remote attestation >=2**
  - This KPI corresponds to the support of the Remote Attestation solution in at least two types of devices among the ones addressed in the project:
    - Smartphone (Domain A and C),
    - Drone (Domain A)
    - Industrial device (Domain B).
  - The support of Remote Attestation in a device refers to:
    - the device's ability to provide Evidence about its state to a Verifier
    - the ability for a Verifier to properly generate an Attestation Request, including the set of Claims to be attested.
  - In the scope of P1, the following use cases contribute to its evaluation:
    - UC A3 (section 3.2.3) and UC C2 (section 3.4.2) - these refer to the support of RA in a smartphone (concretely, running Android OS).
  - The other types of devices are planned to be supported in P2.
  - To accomplish this KPI, RA's Attester runs on the device in the background, communicating regularly with the RA's Verifier (located on in a remote server), sharing relevant device information (in P1, this is dummy/test data).
- **Types of IoT devices reputation affected by RA >=1**
  - This KPI corresponds to the capability of the Verifier to transmit Attestation Results which a Reputation System will compute, and which may affect a device's

reputation.
    - This KPI directly depends / builds on the previous one, additionally depending on the following features:
        - The ability for the Verifier to generate Attestation Results based on received Evidence
        - The ability for the Reputation System to process / appraise Attestation Results (which may lead to updates in the Reputation of a Device)
    - It is not planned for evaluation in P1, considering that both developments are planned for the scope of P2
- **Number of IoT services reputation affected by RA >=1**
    - This KPI corresponds to the capability of the Verifier to transmit Attestation Results which a Reputation System will compute, and which may affect a service's reputation. It thus refers to the specific case of attesting a Drone; being under the responsibility and control of the IoT service provider, the Attestation of a Drone should contribute to both the device (i.e., the drone) and the associated service (DGA) reputation.
    - This KPI directly depends / builds on the previous one, additionally depending on the following features:
        - The ability for the Verifier to generate Attestation Results based on received Evidence
        - The ability for the Reputation System to process / appraise Attestation Results (which may lead to updates in the Reputation of the associated service).
    - Similarly, to the previous KPI, it is not planned for evaluation in P1

For P1, the evaluation of the first KPI above will focus on the basic functionalities of the Attester on the smartphone using dummy data, guaranteeing that the Attester runs and communicates successfully with the Verifier. This is the required to guarantee that remote attestation as a whole is working properly. Further work, in P2, will be concerned with using real data from the device. Additionally, also in P2, the Attester will be integrated in drone, running on a Linux environment.

With respect to the remaining KPIs, even though they are planned for P2, work is underway regarding the specification of communication processes and message formats between Remote Attestation and the Reputation System.

4.3.10 Reputation System KPIs

For P1, the Reputation System component will be involved in the A1, A2, A3, B1 and C2 use cases. In all the use the cases the reputation system will receive information from components and will determine the reputation score, in the respective exchange. The reputation system shares reputation in the *reputation_update* exchange, regarding the respective entities.

The KPIs associated with P1 in the reputation system include:

- **Types of entities supported (persons, devices, services) >= 3**
  In the domain A use, case the reputation system supports the *devices*, *entities* and *services*. The types of entities are determined on the registration process. In domain B the *constrained_devices* are considered, while on domain C, the persons and devices are supported. The information provided in the registration conveys relevant information like the identifier and the type of entity.

- **Time to process an event < 1 second**
  The reputation system was built with support for data pipelines that allow to process events in a scalable fashion. These pipelines rely on the spark framework.

- **Number of messages analysed by time unit: 10 per second**
  The reputation system was built with support for data pipelines, that allow to parallelize the process events in a scalable fashion. Through the spark framework, the processing can occur based on the exchange where events are received.

5 LEGAL COMPLIANCE SPECIFICATION

5.1 Overview of Legal Considerations

The ARCADIAN-IoT project aims to promote innovative, decentralised solutions for trust and identity management in IoT systems, by considering all the entities interacting with such systems, including persons, IoT devices (objects) and respective applications/services.

The design of such technologies, the interaction of the same and, above all, their use in P1 raises questions which are specifically governed by several European regulations (and member state legislations) including, *inter alia*, the processing of personal data.

The purpose of this section is to identify, for each relevant Domain, the main relevant legal concerns and, against this background, outline the applicable regulatory framework.

Once the relevant regulatory framework has been defined, considerations will be made with regard to ARCADIAN IoT's compliance with the requirements set out by the applicable legislation and, on the basis of these considerations, conclusions on legal validation will be made.

5.2 Domain Legal Concerns

The key legal issues on the Domains concern the protection and fair sharing of personal data processed to offer the services, since these involve the use of cutting-edge technologies (e.g., AI, facial recognition, IoT) capable of significantly affecting individuals with regard to their personal data, including sensitive data.

According to the accountability principle enshrined in EU Regulation 2016/679, those who determine the means and purposes of a personal data processing operation (data controllers) and those who practically perform it (data processors) are responsible for ensuring full compliance with data protection principles and rules. This must be done by considering the specific context of the processing, and by taking any measures deemed appropriate on a case-by-case basis.

Even if the services and tools developed in the context of Arcadian-IoT will be simply offered on the market and, therefore, will be used by third parties for their own processing purposes and under their own responsibility, the Partners involved are required to design, develop and distribute systems and models that allow said third parties to process personal data in accordance with the rules in force.

Fundamental principles such as data minimisation, purpose and storage limitation, lawfulness, fairness, transparency, and security must therefore govern every hypothesis considered, right from the design of the processing activities, and by default.

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

With reference to Domains A and B, some technologies used by the partners (*i.e.*, blockchain, AI, biometric technologies and IoT medical devices and drones) might raise issues on data protection, already detailed in the D2.1.

Also of some relevance is Article 5(3) of Directive 2002/58/EC, applicable to situations where an IoT stakeholder stores information or gains access to information stored in an IoT device, to the extent which the IoT devices in question qualify as “terminal equipment” pursuant to this provision. The Article in question provides, as a condition of lawfulness, that the subscriber or user gives

his/her consent to the storage of and access to his/her data, unless these actions are "strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".

Although many of the legal concerns taken into consideration in the evaluation of project pilots have already been addressed in D2.1, in the following paragraphs a brief description of them will be given for an easier understanding of the considerations made in this deliverable.

IoT and blockchain components are used across all Domains. The facial recognition system and drones, on the other hand, are only used within Domain A. Other points of interest are the use of AI systems, appropriate assessments of data retention and deletion, as well as the easy exercise of data subjects' rights.

5.3 The Regulatory Framework

The relevant legal framework for this deliverable is the Regulation (UE) 2016/679 on the protection of natural persons with regard to 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 European authorities and bodies, namely:

- the Opinion 8/2014 on the "*Recent Developments of the Internet of Things*" 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 HighLevel 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 communications* or "***ePrivacy 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.

5.4 ARCADIAN IoT Compliance Considerations

5.4.1 Domain A

Regulation (EU) 2019/947 emphasises that all drone operators and remote pilots - used within the Domain A - must comply with European and national rules regarding privacy and data protection. Drone operations must be carried out with the minor interference with privacy and personal data of individuals, and any personal data collected must be handled in compliance with the principles, requirements and data subject rights laid down in the GDPR.

The use of AI systems entails risks that have the potential to undermine the fundamental rights and freedoms of individuals, including the lack of comprehensive and transparent information about how the technologies work, or the lack of human intervention and control in the automated process. Furthermore, many concerns relate to the technical robustness of the system, the confidentiality of the data processed, as well as the non-discrimination and fairness of the processing.

Along the lines of what will be provided for in the text of the AI Act, which will be approved by the end of April 2023, the GDPR imposes further safeguards in the case of use of AI systems in the processing of personal data. The main requirement in this sense, in accordance with the transparency principle and with the validity of consent, is represented by the provision of a suitable information notice to users.

In fact, the consent of data subjects to the processing of their data must be free, specific, informed and unambiguous, and these requirements could be compromised in the face of the use of AI technologies that need to be explained to the user. For this reason, the AI Act will require the provision of specific information on the functioning of the AI, on the levels of accuracy, robustness and cybersecurity, as well as on the instructions for the correct use of the system. Only by providing such detailed information, the consent received from the user will be fully valid.

As regards fully automated decision-making processes that can significantly affect individuals, pursuant to art. 22 of the GDPR, data subjects have the right not to be subject to such decisions, unless the related data processing is based on the fulfilment of a contract, or on a legal authorisation, or on the explicit consent of the data subject.

In any event, however, data controllers shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. In addition, such decisions shall not be based on special categories of personal data, unless the processing is based on the explicit consent of the data subject.

Within the ARCADIAN-IoT framework, AI components are used, *inter alia*, for facial recognition purposes in Domain A.

The use of facial recognition systems implies the processing special categories of personal data pursuant to Article 9 of the GDPR. Therefore, particular concerns relate to the processing of such categories of data, for which the GDPR calls for specific and additional safeguards. In particular, the processing of such categories of data makes it particularly crucial to identify an appropriate legal basis, which in this case can be identified in the consent of the data subject pursuant to Article 9(2)(a) of the GDPR.

Once the informed, free, specific, and unequivocal consent of the user concerned has been obtained, the processing of his or her data may be deemed lawful. However, for the purpose of identifying the user, the drone must compare his/her facial features with those of other people who might be nearby, and thus also process their biometric data. Unlike the user, these individuals have not received adequate information about the processing of their data, nor have they given their consent to the processing.

In the EDPB Guidelines on video surveillance, this is interpreted to mean that, although any other individuals filmed are not identified, their biometric data are nevertheless processed, through comparison, to uniquely identify the relevant user/data subject. As a result, "*an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera*". It is also recommended to offer, for authentication purposes, "*an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject*".

An identical principle is also provided in the EDPB Guidelines on Virtual Voice Assistants, with regard to the unique identification of users of such devices through the comparison of their voice templates (which are biometric data as well). Also in this context, the EDPB requires data controllers to "*offer an alternative identification method to biometrics*".

As regards the measures suggested and recommended by the two Guidelines, the EDPB highlights the following:

- in compliance with the **data minimization** principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing, and provide default settings that limit any data collecting and/or processing to a minimum required amount needed to provide the service;
- it is essential to ensure **full transparency of information** on data processing, in particular, on where biometric identification is used and how biometric models are stored and propagated across devices;
- in accordance with the **security principle**, it is fundamental to take all necessary precautions to preserve data availability, integrity and confidentiality, by identifying the most appropriate location for the storage of facial templates of the user and related data (especially by providing segregation measures which keep data in separate databases), and by generating, storing and matching such templates exclusively on local devices;
- particular attention must be paid to the **accuracy of the data**, which must be kept up to date, rectified where necessary, and processed so as not to create substantial bias towards different demographic groups;
- **standards** such as ISO/IEC 24745 and techniques of biometric model protection should be thoroughly applied.

As for the legal basis for the processing of third-party biometric data, the EDPB states that "*solutions based on the user's data alone should be given priority. In concrete terms, this means that **biometric recognition is only activated at each use at the user's initiative, and not by a permanent analysis*** (…). *For instance, a specific keyword or question to the persons present could be provided in order to obtain their consent to trigger biometric processing. For example, the user can say "identification", or the assistant can ask "do you wish to be identified" and wait for a positive response to activate biometric processing*".

For more details on legal concerns on this point, please refer to D2.1.

In the context of P1, the aforementioned concerns are addressed, since:

- the AI systems are not used to make decisions about individuals;
- for the purposes of the development of the P1, the Partners use only personal data of volunteers, who, before taking part in the Pilot, have received an information notice in accordance with the Regulation, containing all the information related to the Project and the functioning of the technologies involved; on the basis of this information, volunteers have given their consent to participate and to the processing of their personal data. Therefore, the risk of lack of information and invalid consent is prevented;
- with specific reference to the facial recognition system, the AI system, in its use, is monitored and supervised with human intervention, as well as protected by robust cybersecurity systems, as detailed above; the personal data processed are therefore protected from any loss of confidentiality;
- the data used for training the algorithms for the Pilot are not disclosed outside the Project;
- appropriate technical measures are adopted to ensure the security of the personal data processed.

Moreover, in the P1, the use of drones implying the processing of personal data only takes place with reference to the aforementioned volunteers, since the drones are only used in a space that

is not accessible to the general public, but only to researchers who have reason to access it, as well as to volunteers who have given their consent to participate in the Project.

The use case in Domain A might not give rise to particular concerns in its eventual concrete application either, as long as:

- an information notice containing all the information relating to the processing of personal data, which must be clear and complete but without impairing its accessibility, is provided to the data subject;
- the data subject's consent is requested before processing and, in particular, before capturing biometric data for facial recognition purposes;
- appropriate technical measures are adopted to ensure the security of the personal data processed;
- processed data are divided and stored in separate archives;
- the data are not used for purposes other than those communicated to the data subject;
- for the purpose of unique user recognition, drones use as few facial points as possible;
- drones only start filming and recording when the user has been reasonably uniquely identified;
- human intervention, and the possibility for users to easily request data rectification or deletion are foreseen.

However, a possible issue concerning the use of drones in an unsupervised (i.e., public or publicly accessible) environment must be considered.

In fact, as anticipated, for the purposes of unambiguous identification, the drone could compare the user's biometric template with the facial points of other persons present in the intervention area. The screening of such individuals entails the processing of particular categories of data, which, however, would not be supported by any legal basis, since persons other than the user who has downloaded the application cannot be provided with appropriate information or consent to the processing of their sensitive data.

In this respect, the follow-up to the recommendations of the EDPB will be of crucial importance. In particular, it is considered appropriate to:

- foresee and design – where possible – one or more alternative solutions for the unique identification of the user, which do not involve the processing of biometric data;
- develop a solution that allows biometric recognition at the exclusive initiative of the user and for each individual case of intervention, e.g., through a software command or a confirmation request; and
- raise users' awareness of the correct use of the services, for instance by asking them to locate themselves in uncrowded areas when calling the drone, in order to allow the drone to identify them immediately and without having to compare faces of other individuals.

It is not possible, for the present case, to develop alternatives that do not use biometric recognition, since this is one of the necessary authentication factors envisaged. Nonetheless, facial recognition will not be operated indiscriminately. It will operate only on the specific initiative of the user who requested the drone, after it has reached the place of intervention thanks to the GPS localization and has wirelessly connected to the user's device via the app, and only for the time strictly necessary to confirm the identity of the user. An app notification could ask the user if he intends to proceed with facial recognition and, if so, will provide him with the necessary instructions on where and how to position himself, thus excluding the risk of processing other people's data.

5.4.2 Domain C

The major risks associated with the medical IoT system underlying Domain C relate to the 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 (for more details please refer to D2.1).

As mentioned in the previous paragraph, the processing of such categories of data makes it particularly crucial to identify an appropriate legal basis, which in this case can be identified in the consent of the data subject pursuant to Article 9(2)(a) of the GDPR. Consent must be given in accordance with the requirements of the GDPR, especially when the data being processed relate to minors (see Articles 7 and 8 of the GDPR).

Furthermore, in view of the sensitive nature of the data processed, attention must be paid to the security of the data processed via the IoT system. The remote use of sensors to monitor – in different ways – the user's health could lead to obtaining inaccurate, or even erroneous, data about the data subject, thus invalidating the subsequent steps to be taken based on such data. The systems used, therefore, must be set up in such a way to allow the user to promptly ask the rectification of any incorrect or outdated data, as well as the deletion of such data if deemed possible.

The policies for managing access to such data must also be taken into consideration, bearing in mind that the healthcare facilities that will decide to adopt the services in question may need to guarantee access to such data by, for example, collaborators of the treating doctor, nursing staff, technicians and IT collaborators of the hospital structure. UI of the systems in question should therefore be designed to allow for the customization of access and permission policies.

Amongst data subject rights, particular attention should be paid to that of data portability pursuant to Article 20 of the GDPR, according to which the data subject has the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format, as well as the right to transmit those data to another controller without hindrance. In this sense, it is necessary to evaluate the compatibility and interoperability of IoT devices with the other tools on the market, in order not to compromise the essence of the right in question.

In the context of the P1, all the issues outlined are addressed, since the Partners use only personal data of volunteers, who, before taking part in the Pilot, have received an information notice in accordance with the GDPR, containing all the information related to the Project. On the basis of this information, said volunteers give their consent to participate and to the processing of their personal data. Therefore, the risk of lack of information and invalid consent is prevented. Furthermore, volunteers' personal data are not used for purposes other than those for which they were collected (*i.e.,* the development of the Pilots).

The use case in Domain C does not give rise to particular concerns in its eventual concrete application either, as long as:

- an information notice containing all the information relating to the processing of data carried out through the IoT system is provided to the data subject;
- the data subject's consent is requested before processing (in the case of minors, consent must be given by the parental authority);
- appropriate technical measures are adopted to ensure the security of the personal data processed;

- the data are not used for purposes other than those communicated to the data subject.

5.4.3 The use of blockchain in IoT

IoT hides security concerns that can be addressed by the blockchain, however the use of blockchain involves risks in relation to the GDPR requirements. In particular, the “immutability” of the data, implied in the very nature of the blockchain, constitutes a critical point of tension between such technology and the provisions of the GDPR (for more details please refer to D2.1).

Nevertheless, no personal data are used or stored within the Pilot (and the Project in general) on the blockchain technology used by the Partners. Therefore, all possible tensions between the GDPR and the use of such technology are prevented.

5.5 Summary

The use of such technological components (*i.e.*, blockchain, AI, biometric technologies and IoT medical devices and drones) might raise issues on the applicable law (please see paragraph 5.4 above). However, in the context of P1 all possible concerns are addressed for the reasons stated in paragraph above.

Given that personal data legislation is the main legal framework, it should be also noted that many partners do not use personal data in the development of their own technologies: this is due to the fact that, on the one hand, these are sometimes security systems (e.g., cyber threat intelligence component, encryption algorithms, eSim, *etc.*) that by their very nature do not involve the processing of data and, on the other hand, because in some cases data are processed anonymously. Furthermore, from this perspective, many concerns related to the security of the data are already addressed by the nature of the Project itself, which, as is known, aims precisely at enable decentralised management of trust, identity, privacy and security in IoT systems.

Finally, with regard to the interaction of the components within P1, as already pointed out, all possible concerns are addressed, especially in light of the fact that the Pilot is performed exclusively with volunteer data, who have been informed about the Project, in spaces specifically reserved for Pilots (and thus not accessible to the public).

In their concrete applications, however, only Domains B and C do not raise concerns. Domain A, on the other hand, as anticipated, could present issues where the drone is used in a public space.

With a view to guaranteeing full compliance with data protection legislation, it is also suggested to evaluate the drafting of a Data Protection Impact Assessment (DPIA) pursuant to Article 35 of the GDPR, which makes it possible to obtain a global picture of the circumstances of use of the Domains and the related risks for the rights and freedoms of the persons involved and, consequently, to promptly determine the corrective actions and other security measures suitable for minimizing such risks.

6 VALIDATION AND EVALUATION RESULTS

In this section it is presented the results of the validation and evaluation activities performed by Task 5.5 for the P1 scope. For validation it was considered the Use Cases and scenarios specified in section 3. For evaluation it was considered the KPIs and measurement methods specified in section 4.

6.1 Validation Results - Domain A (Emergency and Vigilance)

6.1.1 Use-Case A1 - *Person registration at the DGA service*

Recalling this use case, it focuses on a DGA end user (physical person), registering in the DGA service integrated with 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). Additionally, the Reputation component integrates with subscribing to the resulting registration event.

Next are presented the validation results as per each step of the use case:

<u>These following actions are required for the validation of Prototype 1:</u>

1. Open DGA App & click on links to Registration & sub-link to be issued with user mobile wallet identity to the user´s SSI Wallet.
    a. Download, Install the SSI Wallet App on mobile & configure Fingerprint access.
    b. Click on link to be issued with a mobile wallet identity, and user resultantly receives an identity in their wallet.

This step was **successfully validated.**

2. Now that the user has a wallet identity, he/she 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 which shows a QR Code and link (to click on if seen on a mobile) to present their mobile wallet identity.
    NOTE: The user is informed to open their mobile wallet before proceeding to click on the link.
    b. The user clicks on link and receives a request on mobile to present their Person Verifiable Credential that was previously issued to them.
    c. The user confirms the presentation.

This step was **successfully validated.**

3. 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.

This step was **successfully validated.**

4. User is asked to provide photo images to finish the registration and the user provides their

images as requested by the app.

This step was **successfully validated.**

5. User is informed on the DGA app that their registration is complete.

This step was **successfully validated.**

6. Registration event is sent to the ARCADIAN-IoT Framework with Person Identity and new aiotID.

This step was **successfully validated.**

7. ARCADIAN-IoT Framework services in P1 (Reputation, Self-Recovery) initialise their respective services for the new aiotID.

This step was **successfully validated** with the reputation system. Other components will follow in upcoming activities.

6.1.2 Use-Case A2 - *Person authentication at the DGA service*

Recalling this use case, it 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, allows 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).

Next are presented the validation results of each step of the use case:

1. The person has a smartphone with the DGA app installed, the SSI Wallet (Ledger uSelf android wallet app), and communicates using cellular networks (e.g., LTE or 5G) with a TRU eSIM/SIM.

This step, that mostly focuses on the pre-conditions was **successfully validated**. The DGA app was ready for the needed functionality, as well as the SSI Wallet, and the device had a TRU eSIM/SIM.

2. Using the DGA app to authenticate, the person will be requested to take a photo. The app will send, in a secure way, to its (DGA) backend, this photo appended to the ARCADIAN-IoT ID it wants to authenticate.

This step was **successfully validated**. All Domain A technologies (app and backend) were ready and performing as expected. However, in P2, this step will be strengthened with the Hardened Encryption component.

3. Communicating through the cellular networks, when the request passes through the core network infrastructure, an ARCADIAN-IoT component (*Notarizer*) appends to the authentication request a signed and protected Network ID token (transparent to the user).

This step was **successfully validated**. Based in core network information about the

subscriber, the *Notarizer* issued a network ID token to be used in steps 5 and 6.

4. The person authentication request follows to the DGA backend services, which, for using ARCADIAN-IoT MFA services, forwards the request to the MFA component.

   DGA services backend behaved as expected. This step was **successfully validated**.

5. The MFA splits the request received, asking: (1) ARCADIAN-IoT's Biometrics component to confirm if 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.

   ARCADIAN-IoT MFA backend behaved as described. This step was **successfully validated**.

6. 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.

ARCADIAN-IoT Biometrics and Network-based authentication components functionally behaved as described. This step was **successfully validated**.

7. The SSI component will establish 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.

ARCADIAN-IoT SSI components functionally behaved as described. This step was **successfully validated**.

8. If the three authentication factors verification is 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, which returns it to the requesting personal device – the person is now authenticated and can proceed with the use of the DGA mobile app.

   ARCADIAN-IoT MFA issued and signed an ID token, which was **successfully returned** to the requester device/app.

9. 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.

The sharing of authentication results is still ongoing. This step was **not validated**.

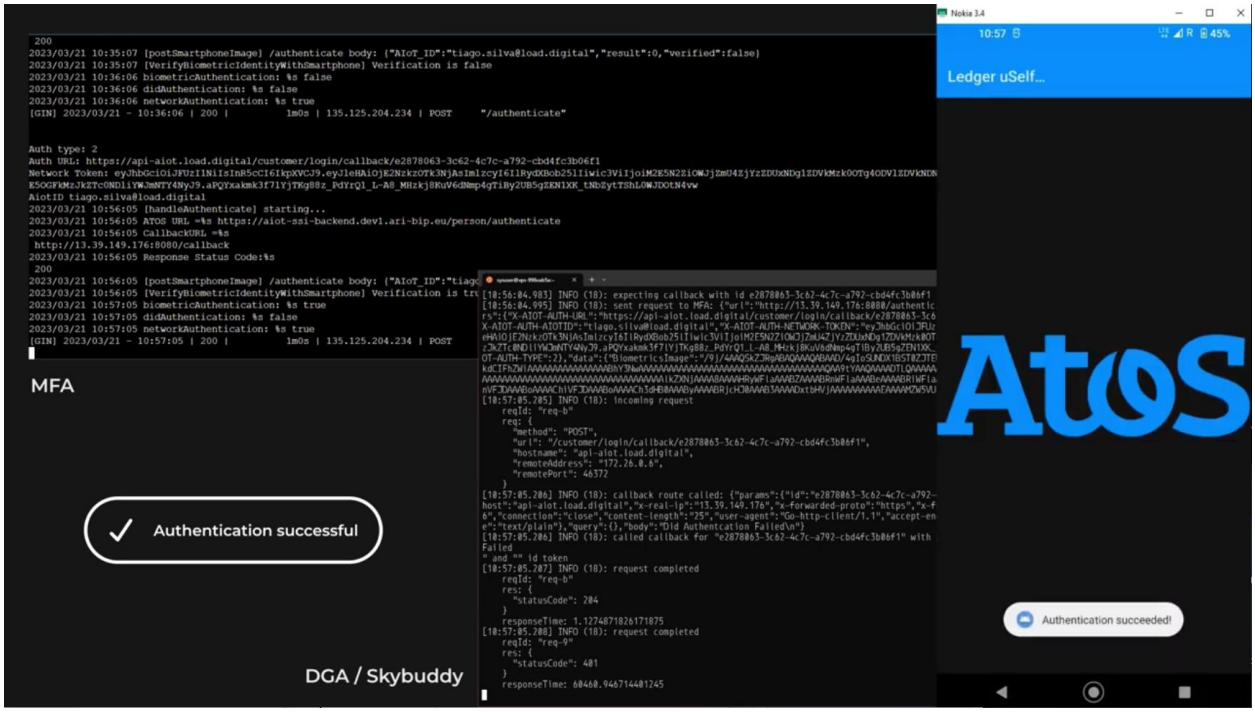

Figure 3 - Screenshot from demo joining the MFA logs (TRU), Ledger uSelf wallet (ATOS) and DGA services logs (LOAD)

This use case allowed to measure KPIs of several components. Functionally the main expected result from A2 was to have a person authenticated using the three authentication factors. This was accomplished. However, the sharing of authentication results to other ARCADIAN-IoT components is still in progress, and there are minor suggestions from the IoT solution provider that will be addressed in the next stage (P2). Considering the agile approach followed, these suggestions are highly valued and welcome.

6.1.3 Use-Case A3 - Person retrieving and editing personal data

Recalling 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. The expected results are the following:

1. Using the DGA App, the person supplies some personal data to the DGA service, which includes name, address, photo, and optional SOS contacts.

This step was **successfully validated**.

2. The DGA service, before providing the requested data to the user, requires reputation information from the user and its personal device.

This step was **partially validated**. The reputation values are used to authorize the personal device to access to the network, and consequently to exchange data with the DGA service. Authorize the access to the network according to the reputation values and reputation policies.

This result has been partially achieved with three types of policies: Policy 1 – block all the traffic between the device and Internet, when the device has a reputation score below a specific value; Policy 2 – Throttle the connection of the device, in terms of bandwidth when the reputation score is below a certain value; and Policy 3 – Device with a reputation score between a certain range cannot communicate with a specific destination. It was **not validated** the use of reputation information from the DGA service.

3. Upon the reputable reputation values, according to the configured policies, the data is retrieved to the personal device of the user in an encrypted way.

This step was **partially validated**, without using the reputation information.

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. If 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.

The integration with the Hardened Encryption is planned for P2. Therefore, this step was **not validated.**

5. The remote attestation procedure is initiated via a manual trigger at the Verifier (running at a remote server)
    a. 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

Successfully validated: The Attester running in a smartphone was able to receive and process the remote attestation request/challenge, retrieving the selected (dummy) claims and nounce. The Attester was then able to securely send - by invoking Hardened Encryption libraries - evidence (set of claims) to the Verifier.

    b. The Verifier displays the received Evidence, which should correspond to the claims displayed at the smartphone side

Successfully validated: The Verifier was able to process the received response, confirming its nounce matches, and appraising the received Evidence against a simple policy (i.e., values match accepted or range of accepted reference values).

6.2 Validation Results - Domain B (Grid Infrastructure Monitoring)

Both **use cases B1 and B2 were successfully implemented**, monitored and documented accordingly. It was practically simulated a failure for each use case, by changing encryption keys in one side (device side or middleware side), in order to enforce the failure of the authentication or of the traffic from IoT devices. There were simulations of failures of Middleware Docker (a stop status, a restart status), and an IoT device fleet simulator was built and executed in order to stress the Behaviour Monitoring component with respect to assessing anomalies associated with fleet events.

A drive test by highspeed train, to stress the hardened encryption system by crypto chip against network availability and bandwidth, was also performed and is shown in Figure 4 and Figure 5.

Figure 4 - Domain B devices (one is equipped with GSM and one equipped with LTE extension communication boards)

Figure 5 - Domain B devices and a power analyser interfaced as grid sensor; monitored electrical power belongs to train passengers' distribution system

6.2.1 Use-Case B1 – New Device Registration

The Use-Case scenario used during P1 Validation is described in section 3.3.1. The validation results for the considered actions are detailed below.

1. Turn on an unregistered device with compiled firmware previously loaded

Validation status: passed

2. Connect with O&M set-up kit on device and from device firmware configuration CLI (command line interface), by local logging to device with BOX2M provided user and password, and using a local encryption method (“OTS – over the serial”)

Validation status: passed

2.1. Install eSIM or SIM profile (APN name, user, password), depending by chosen SIM type

Validation status: passed

2.3. Set-up the communication module type (GSM, UMTS, LTE, LTE-M, NBIoT, 5G, ETH, WiFi, ETH & WiFi)

Validation status: passed

2.4. Set-up the communication failover option (if the device is equipped accordingly, with specific communication extension board)

Validation status: passed

2.5. Set-up Device ID, user and password

Validation status: passed

2.6. Set-up Middleware contact point (telemetry broker address - domain name, port number)

Validation status: passed

2.7. Call encryption keys generation function, defined into crypto chip library by crypto chip vendor (Infineon), which is part of device firmware libraries, to randomly generate keys for authentication, traffic and recovery stages

Validation status: passed

2.8. Take note of the keys (optimally not on electronic devices, to do not leave traces which may be a vulnerability point), to be defined into Middleware side too; destroy the notes after

Middleware definition; every time when it takes place another new device registration, make sure the randomly generated keys are unique (by comparing with previous defined ones);

Validation status: passed

2.9. Activate the log monitor on a terminal application of O&M laptop, keeping device connected

Validation status: passed

3. Connect to Middleware frontend address and login

Validation status: passed

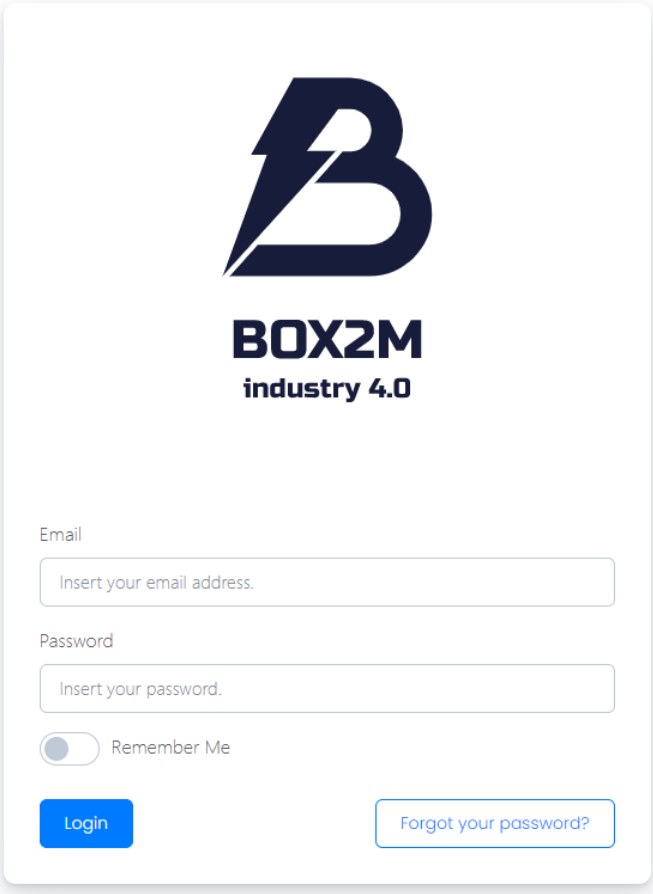

Figure 6 - Middleware login – 1st authentication step

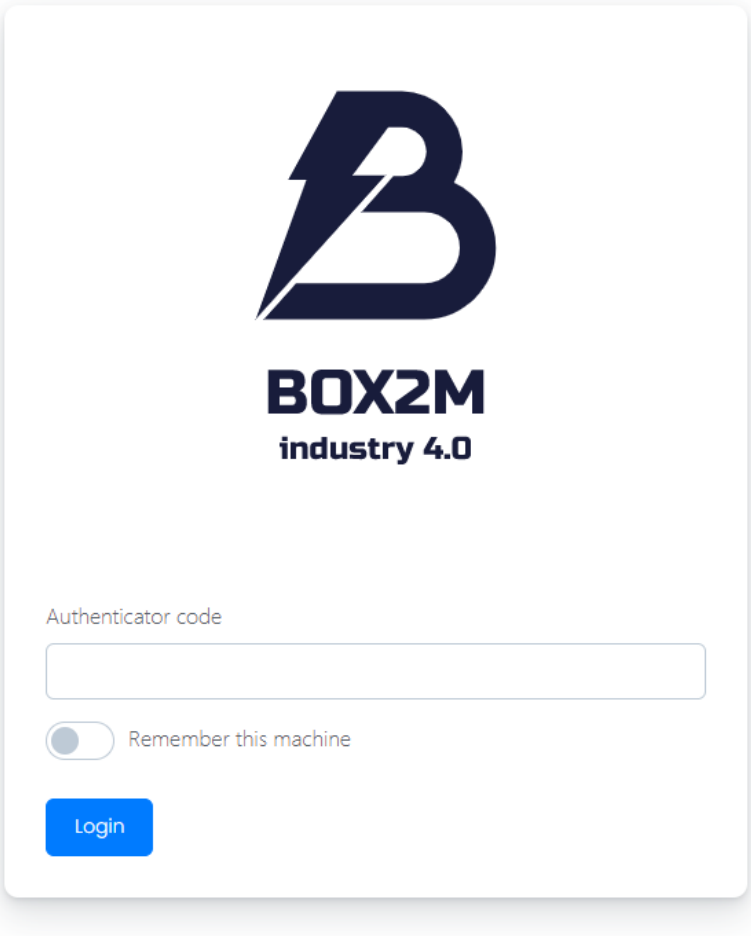

Figure 7 - Middleware login – 2nd authentication step

3.1. Into “Devices” menu, “General” sub-menu, define new device, with the ID, user and password used into 2.5., check mark the options “Show in reports” and “Is enabled”.

Validation status: passed

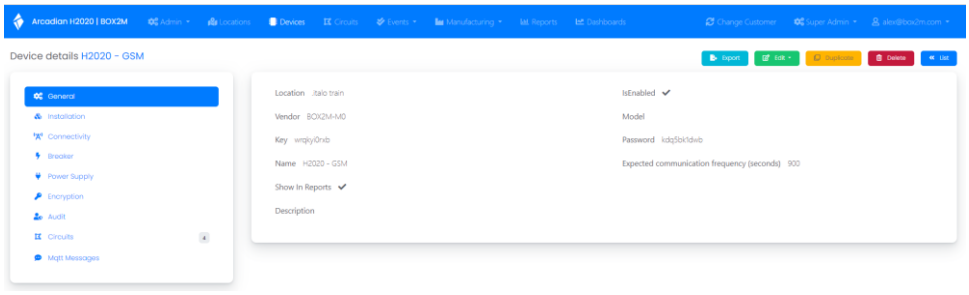

Figure 8 - Middleware admin page – Devices sub-menu

3.2. Into “Devices” menu, “Encryption” sub-menu, define “Use Key 1” with the value generated at 2.7. for authentication, “Use Key 2” with the value generated at 2.7. for traffic, “Use Key 3” with the value generated at 2.7. for recovery

Validation status: passed

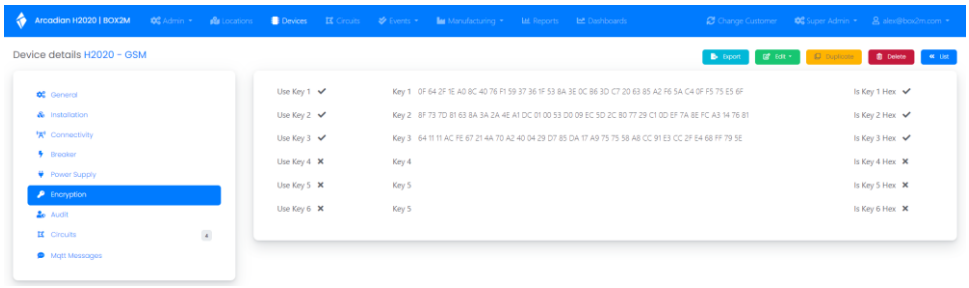

Figure 9 - Middleware admin page – Devices sub-menu – Encryption

3.3. Set-up the behaviour monitoring function (which was hardcoded into Middleware, not by GUI/front end), for both Docker containing the Middleware and for the new provisioned device. Every time when a new device is added into fleet, it must be defined into behaviour monitoring too. Every time when an existing device is removed from fleet, it must be erased from behaviour monitoring too

Validation status: passed

3.4. Set-up the connection with Message Bus of the ARCADIAN-IoT Framework (in order to send messages to the Behaviour Monitoring System)

Validation status: passed

3.5. Publish device ID (i.e., ARCADIAN-IoT ID) to Device Behaviour Monitoring (DBM) and to the Reputation System via the dedicated exchanges/queues

Validation status: passed

3.6. Configure the relaying of devices' authentication events to the Device Behaviour Monitoring (DBM)

Validation status: passed

3.7. Configure the periodic push (i.e., every 30 seconds) of aggregated system calls (associated to the Middleware's container) to Device Behaviour Monitoring (DBM)

Validation status: passed

4. Connect the device to sensors kit, power up sensors, reset the device and monitor: **passed**

Justification if not passed: hardware failure

4.1. on terminal application of O&M laptop, the settings done between 2.1. to 2.7. to be

kept as defined

Validation status: passed

4.2. On terminal application of O&M laptop, the success or failure state of device connection to network operator data services

Validation status: passed

```
Data over GPRS GSM
Time to send: at interval in minutes, interval: 3 minutes
Use: E-SIM
Modem is OFF, power on Modem
Modem is Ready
IMEI: 869640057210166
OK read IMEI
Status E-SIM OK
IMSI: 208090063126478
OK read IMSI
OK level signal: 24.0
```

Figure 10 - GSM Technology & eSIM

```
Start GSM Service
OK registered sim
OK data service
OK close the connection MQTT with the server GPRS
```

Figure 11 - GSM Technology & eSIM confirmations

```
Data over LTE
Time to send: at interval in minutes, interval: 3 minutes
Use: SIM
Modem is OFF, power on Modem
Modem is Ready
IMEI: 860537061871414
OK read IMEI
Status SIM OK
IMSI: 208090082636208
OK read IMSI
OK level signal: 16.99
```

Figure 12 - LTE Technology & Regular SIM

```
Start GSM Service
OK registered sim
OK data service

APN USE: iot.truphone.com
```

Figure 13 - Network Credentials

4.3. On terminal application of O&M laptop, the success or failure state of device connection into Middleware telemetry broker

Validation status: passed

AES 256, CBC encrypt

User encrypt:

0000 30 35 30 46 43 44 38 37 31 42 43 34 37 42 44 42 050FCD871BC47BDB

0010 36 45 30 34 41 37 42 42 41 44 33 33 45 33 46 44 6E04A7BBAD33E3FD

AES 256, CBC encrypt

Password encrypt:

0000 38 44 44 31 38 44 30 30 42 31 34 33 35 35 33 42 8DD18D00B143553B

0010 39 43 37 46 44 46 33 46 32 37 45 46 43 42 45 46 9C7FDF3F27EFCBEF

The connection to the MQTT broker was successfully opened LTE

Topic LTE: device/q556p5qgfq

Rx from declare first time Topic

0000 0D 0A 4F 4B 0D 0A 0D 0A 2B 43 4D 51 54 54 53 55 ..OK....+CMQTTSU

0010 42 3A 20 30 2C 30 0D 0A B: 0,0..

OK open MQTT connection to server

1.3. On Middleware SOC (service operation centre), into “Devices” menu, “MQTT messages” sub-menu, either “MQTT Messages” option (for real time, processed messages), or “MQTT messages raw” option (for real time, not processed messages), the success or failure state of device connection to Middleware telemetry broker

Validation status: passed

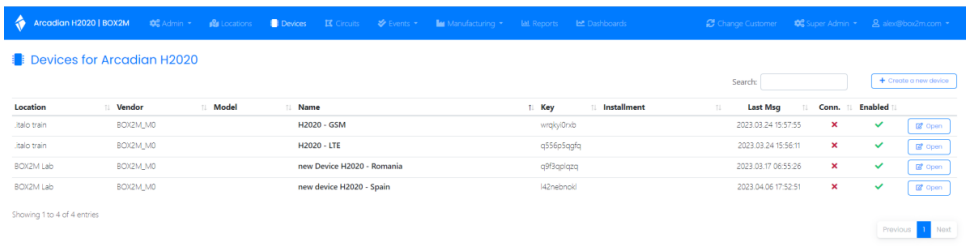

Figure 14 - Middleware admin page – SOC (Service Operations Centre)

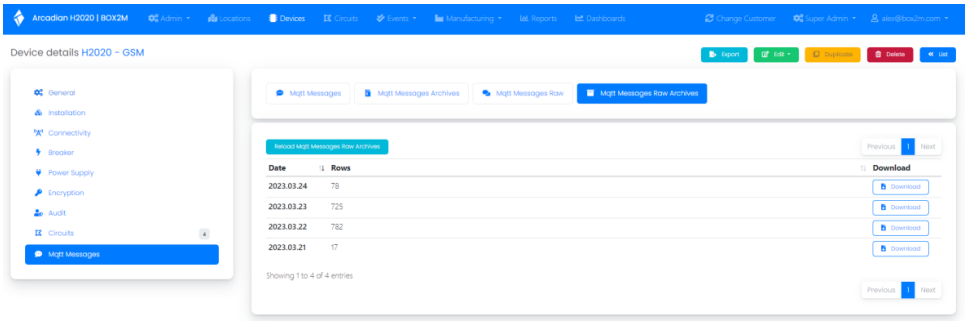

Figure 15 - Middleware admin page – SOC (Service Operations Centre) - debugging messages

{"CustomerId":"c30c6b26-e2db-4cdf-3eac-08da94f5bd68","LocationId":"e5ceffc2-07c9-4e1b-0178-08db2c6b4d60","DeviceId":"5848e4f8-58db-43e0-10bf-08db27ab0f63","MessageType":2,"Username":"q556p5qgfq","ClientId":"q556p5qgfq","Topic":"**Connected**","Payload":"Connected | Client q556p5qgfq | Username q556p5qgfq | Protocol V310","Accepted":true,"Validated":true,"Id":"9c2b9d42-155d-4c90-9237-04f55e9a1d88","TransactionId":"baebe2aa-f210-4677-a257-b4f250a06c45","MachineName":"box2m-messages-service-6b98978bb4-sch55","Timestamp":"2023-03-24T13:46:21.2484316"}

{"CustomerId":"c30c6b26-e2db-4cdf-3eac-08da94f5bd68","LocationId":"407986d1-11f5-4442-7ecc-08da94f5ce36","DeviceId":"5848e4f8-58db-43e0-10bf-08db27ab0f63","MessageType":3,"Username":"","ClientId":"q556p5qgfq","Topic":"**Disconnected**","Payload":"Disconnected | Client q556p5qgfq | Type Clean","Accepted":true,"Validated":true,"Id":"c9d6cfd8-b549-4b07-be1a-05a5c81ccf71","TransactionId":"16b1613a-5cdc-4295-8d13-10c9fe9093d2","MachineName":"box2m-messages-service-6b98978bb4-7b5h9","Timestamp":"2023-03-24T13:20:45.2941737"}

1.4. Forward messages to the Behaviour Monitoring System to enable monitoring and perform post reporting (per certain criteria) of associated events:

Validation status: passed

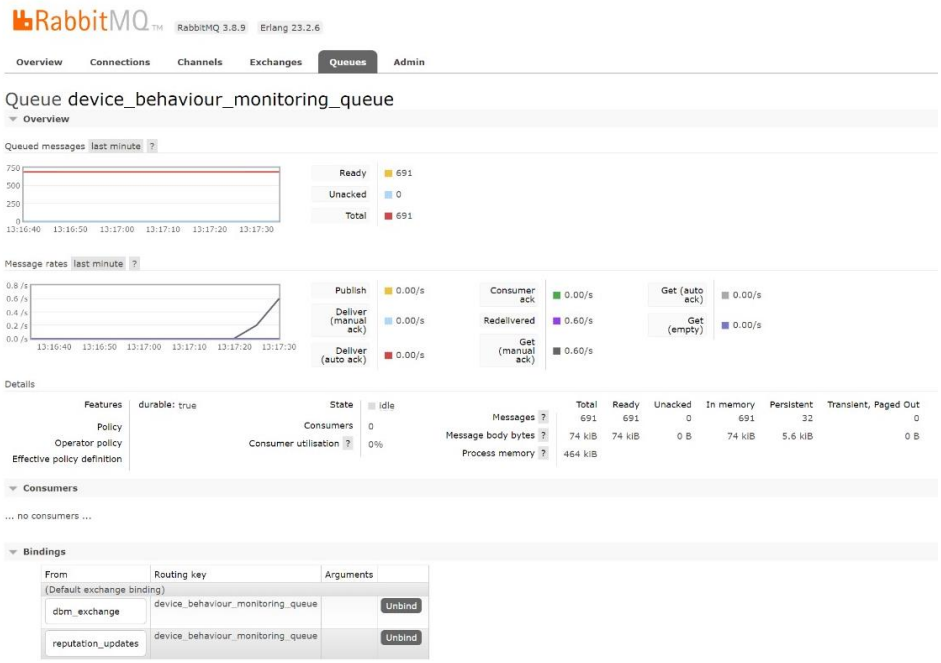

Figure 16 – RabbitMQ admin page – Message queue

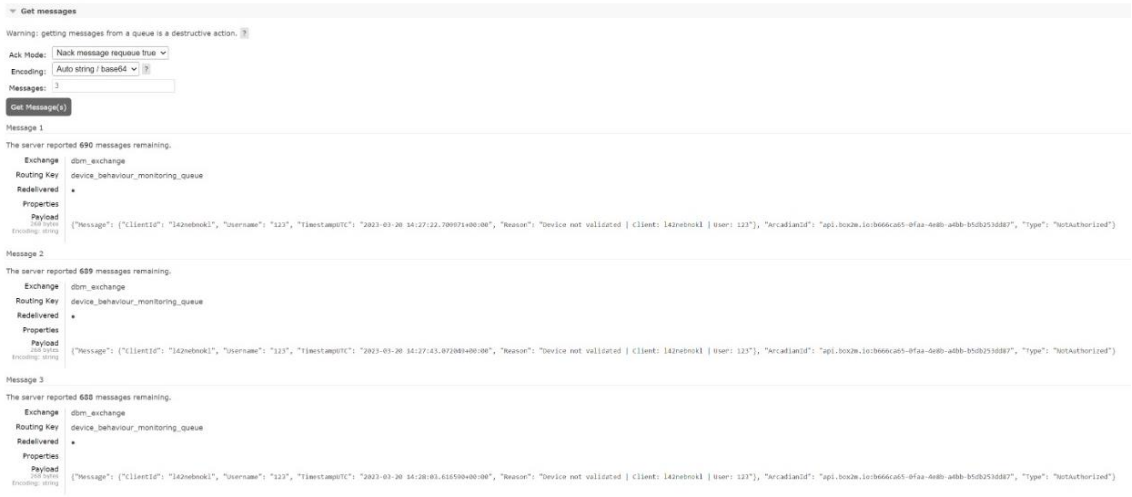

Figure 17 - RabbitMQ admin page (Device “not authorised” event)

Figure 18 - RabbitMQ admin page (Device “connected” & “disconnected” event)

6.2.2 Use-Case B2 - GMS IoT device data gathering and transmission process

1. Turn on an unregistered device:

Validation status: passed

2. Connect with O&M set-up kit on device and from device firmware configuration CLI (command line interface), by local logging to device with BOX2M provided user and password, and using a local encryption method (“OTS – over the serial”):

Validation status: passed

2.1. set-up the circuits ID's:

Validation status: passed

2.2. set-up for each circuit the parameters ID's:

Validation status: passed

2.3. set-up for each parameter the frequency sampling rate of transmission:

Validation status: passed

2.4. activate the log monitor on a terminal application of O&M laptop, keeping device connected:

Validation status: passed

3. Connect to Middleware frontend address and login:

Validation status: passed

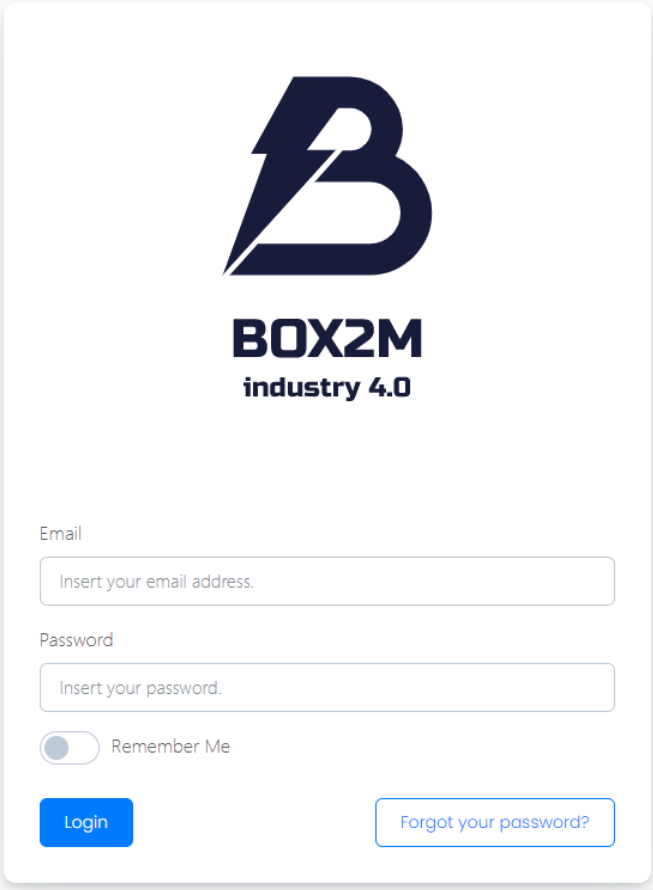

Figure 19 - Middleware login – 1st authentication step

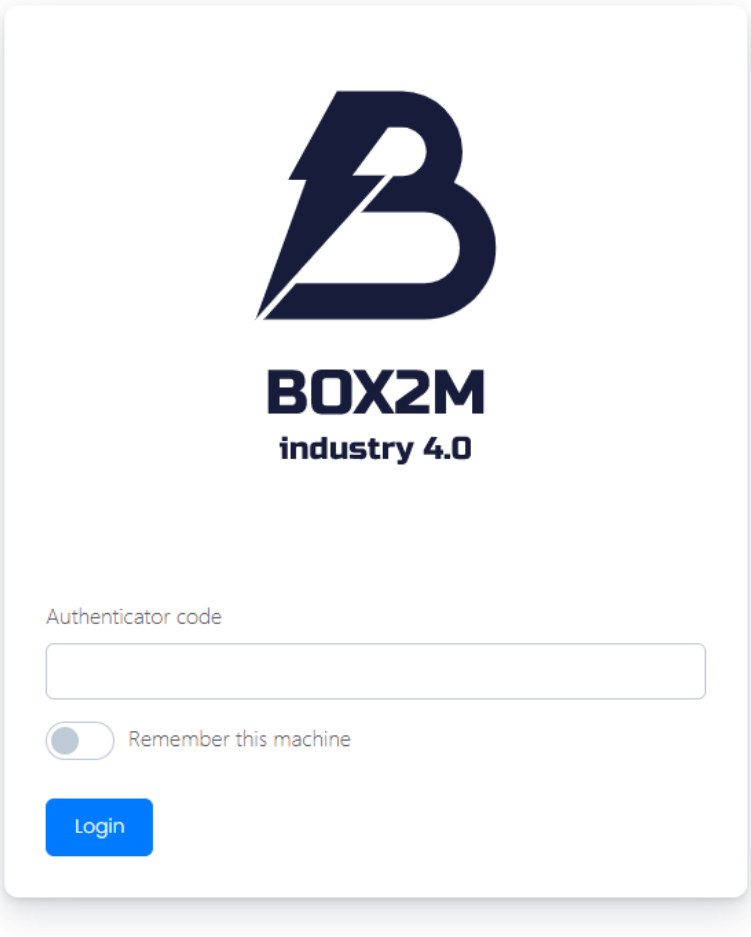

Figure 20 - Middleware login – 2nd authentication step

a. Into “Devices” menu, “Circuits” sub-menu, define new circuits, one by one, for each with their IDs and parameter IDs:

Validation status: passed

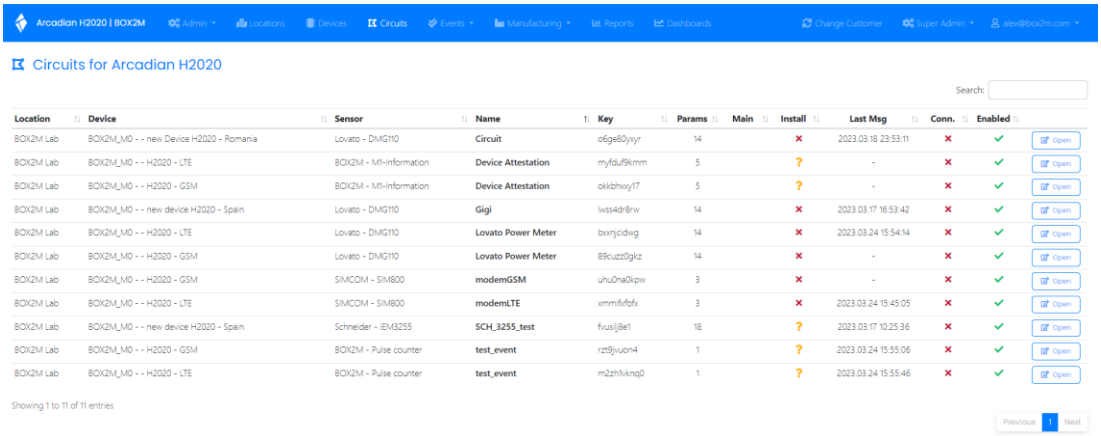

Figure 21 - Middleware admin page – Circuits sub-menu

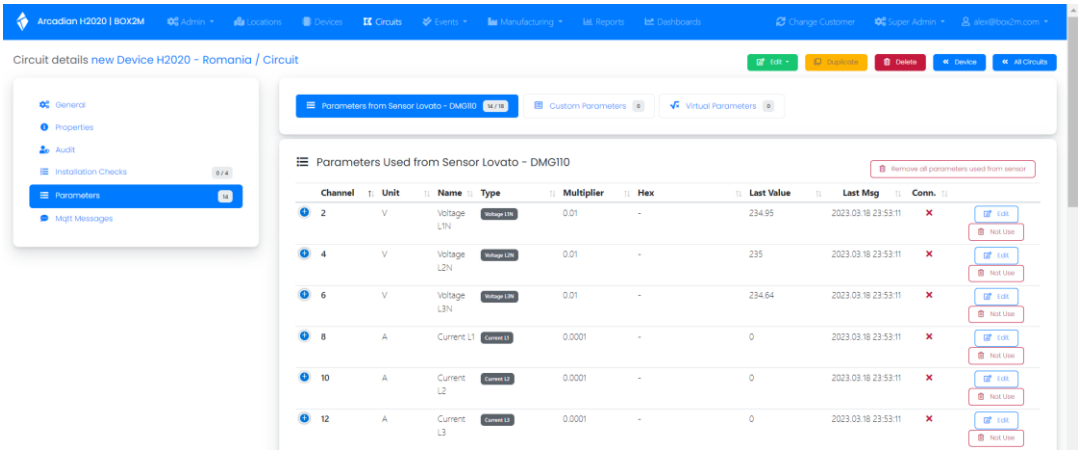

Figure 22 - Middleware admin page – Circuits sub-menu - Parameters

8. Connect the device to sensors kit, power up sensors, reset the device and monitor:

Validation status: passed

a. on terminal application of O&M laptop, the settings done between 2.1. to 2.3. to be kept as defined:

Validation status: passed

4.2.1. on terminal application of O&M laptop, the network operator authentication success and data bear allocation:

Validation status: passed

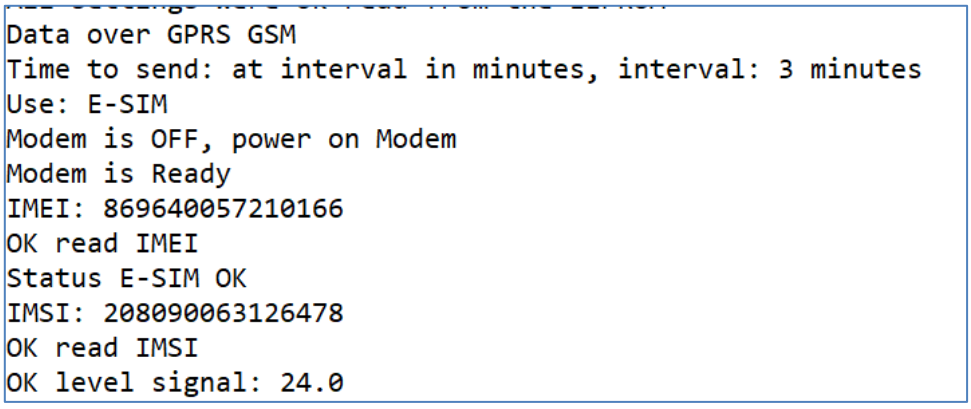

Figure 23 - GSM Technology & eSIM

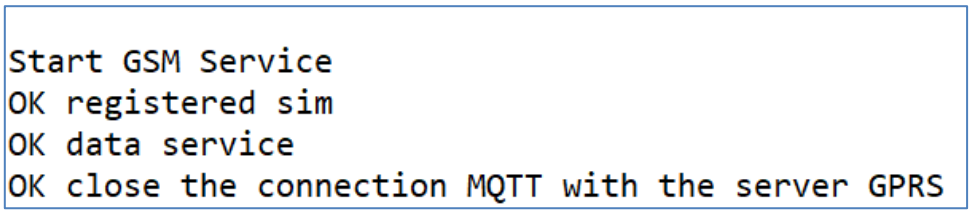

Figure 24 - GSM Technology & eSIM confirmations

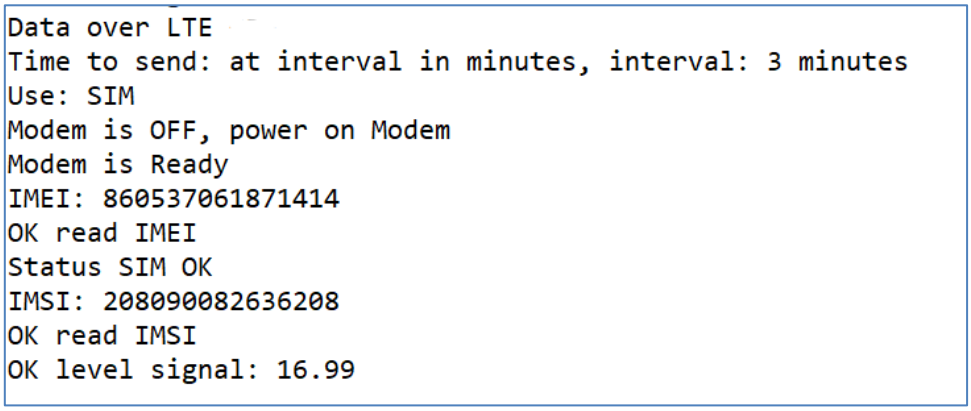

Figure 25 - LTE Technology & Regular SIM

Figure 26 - Network Credentials

4.2.2. on terminal application of O&M laptop, the Middleware telemetry broker encrypted authentication success:

Validation status: passed

AES 256, CBC encrypt

User encrypt:

0000 30 35 30 46 43 44 38 37 31 42 43 34 37 42 44 42 050FCD871BC47BDB

0010 36 45 30 34 41 37 42 42 41 44 33 33 45 33 46 44 6E04A7BBAD33E3FD

AES 256, CBC encrypt

Password encrypt:

0000 38 44 44 31 38 44 30 30 42 31 34 33 35 35 33 42 8DD18D00B143553B

0010 39 43 37 46 44 46 33 46 32 37 45 46 43 42 45 46 9C7FDF3F27EFCBEF

The connection to the MQTT broker was successfully opened LTE

Topic LTE: device/q556p5qgfq

Rx from declare first time Topic

0000 0D 0A 4F 4B 0D 0A 0D 0A 2B 43 4D 51 54 54 53 55 ..OK....+CMQTTSU

0010 42 3A 20 30 2C 30 0D 0A B: 0,0..

OK open MQTT connection to server

4.2.3. on terminal application of O&M laptop, the success or failure of encrypted – with key 3 / traffic type - payload transmission of the previously defined circuits and parameters, on the previously defined frequency rate:

Validation status: passed

Create message no: 1 for circuits type: Local Counter

Check if the local counter is set

Message:
0123456789ABCDEF{"vbat":3.11,"ts":1679583054761,"values":{"xmmifxfbfx":{"10":860537061871414,"20":208090082636208,"40":16.99},"myfduf9kmm":{"100":1.0.19,"101":2023-03-20,"102":M1,"103":ON,"104":BOX2M},"m2zh1vknq0":{"1":0}}}

Message length: 223 - 1

AES 256, CBC encrypt

0000 F5 32 48 F6 F1 A0 42 94 B4 66 41 CD C6 D2 F9 9E .2H...B..fA.....

00D0 79 8B 89 3A 7D 99 B9 25 5C 91 20 3B D8 DA D3 90 y..:}..%\. ;....

Processing the encrypted message

0000 46 35 33 32 34 38 46 36 46 31 41 30 34 32 39 34 F53248F6F1A04294

01B0 35 43 39 31 32 30 33 42 44 38 44 41 44 33 39 30 5C91203BD8DAD390

END processing the encrypted message, len: 448

0000 0D 0A 4F 4B 0D 0A 0D 0A 2B 43 4D 51 54 54 50 55 ..OK....+CMQTTPU

0230 33 39 30 0D 0A 2B 43 4D 51 54 54 52 58 45 4E 44 390..+CMQTTRXEND

0240 3A 20 30 0D 0A : 0..

Process the information received from the MQTT LTE server

MQTT message sent successfully LTE

4.3. Anytime device reboots / restarts, the whole encryption process is retaken from scratch (including authentication); else, if device stays powered, and network operator infrastructure maintains the data connection, and Middleware closes a traffic session, than when another traffic session is started by device, another encryption session for traffic will be started (using again Key 3 as reference for crypto chip to perform the payload encryption); these will be showed explicitly into terminal logger, firmware being designed for this local debugging / monitoring purpose too; obviously, showed data is not in clear, being output just the encrypted string.

Validation status: passed

b. on Middleware SOC (service operation centre), into “Devices” menu, “MQTT messages” sub-menu, either “MQTT Messages” option (for real time, processed messages), or “MQTT messages raw” option (for real time, not processed messages), the success or failure state of device traffic transmission to Middleware telemetry broker and IoT platform; if encryption key do not match with provisioned data, these will be showed explicitly into message in this sub-menu option;

Validation status: passed (middleware front end messages reflecting the settings and / or status, as described previously.

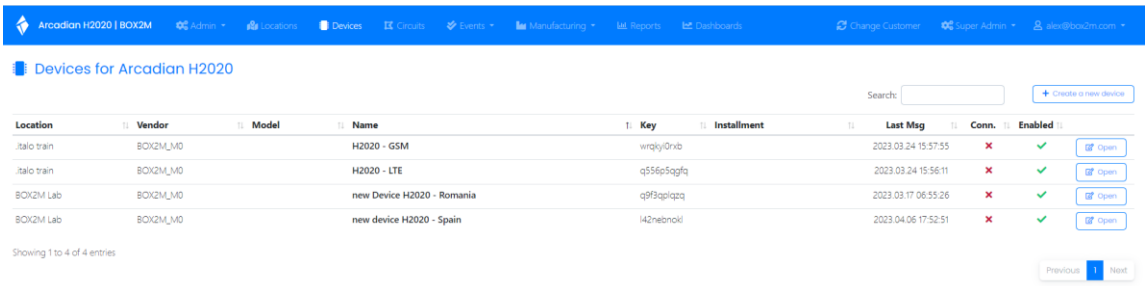

Figure 27 - Middleware admin page – SOC (Service Operations Centre)

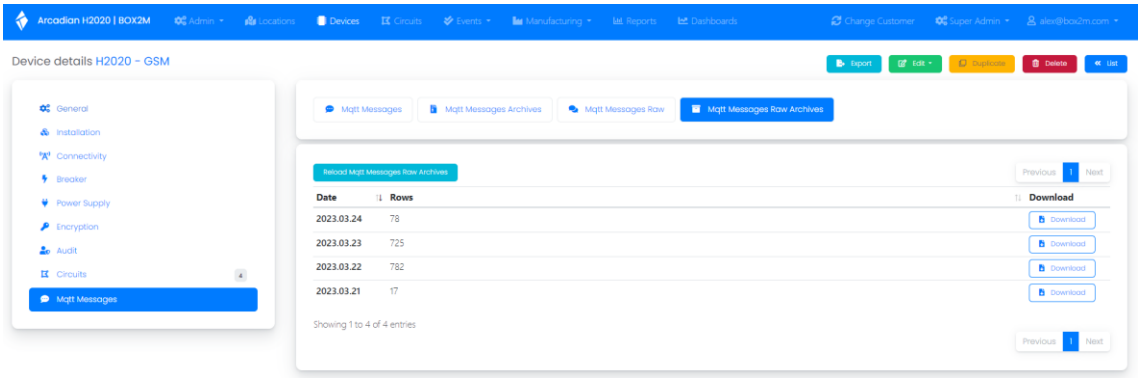

Figure 28 - Middleware admin page – SOC (Service Operations Centre) - debugging messages

{"CustomerId":"c30c6b26-e2db-4cdf-3eac-08da94f5bd68","LocationId":"e5ceffc2-07c9-4e1b-0178-08db2c6b4d60","DeviceId":"5848e4f8-58db-43e0-10bf-08db27ab0f63","MessageType":2,"Username":"q556p5qgfq","ClientId":"q556p5qgfq","Topic":"**Connected**","Payload":"Connected | Client q556p5qgfq | Username q556p5qgfq | Protocol V310","Accepted":true,"Validated":true,"Id":"a1a20156-1272-4756-9b82-062d2820ae9e","TransactionId":"2a4b7c85-6339-4bca-abfe-c2b69533d52a","MachineName":"box2m-messages-service-6b98978bb4-7b5h9","Timestamp":"2023-03-24T13:43:13.1892249"}

{"CustomerId":"c30c6b26-e2db-4cdf-3eac-08da94f5bd68","LocationId":"407986d1-11f5-4442-7ecc-08da94f5ce36","DeviceId":"5848e4f8-58db-43e0-10bf-08db27ab0f63","MessageType":3,"Username":"","ClientId":"q556p5qgfq","Topic":"**Disconnected**","Payload":"Disconnected | Client q556p5qgfq | Type Clean","Accepted":true,"Validated":true,"Id":"d722648f-9c2a-4a20-b09b-068e7f575fdf","TransactionId":"18356eba-378a-4c4a-821f-c343f3500b00","MachineName":"box2m-messages-service-6b98978bb4-2qnq2","Timestamp":"2023-03-24T13:01:25.0491671"}

c. Forward messages to the Behaviour Monitoring System to enable monitoring and perform post reporting (per certain criteria) of associated events:

Validation status: passed - These are similar to the previous section (Use Case B1) in point 4.4.

Same result as previous section (Use Case B1) in point 4.4.

6.3 Validation Results - Domain C (Medical IoT)

6.3.1 Use-Case C2 - MIoT capturing and sending vital signs and perceived health status

In the following we report the validation of the use case involving collecting and storing a patient's vitals, from device to Telemedicine service, with hardened encryption applied to the data in transit.

The following actions are taken into account for validation:

1. Device collects patient vitals. Justification if not passed: failure to collect vitals due to device malfunction (Firmware, hardware, ...)

   Example data:

   {

   "timestamp":1679656096635,

   "session_type":"SPO2",

   "chart_patient":4,

   "chart_session":12,

   "data":"[167, 165, 162, 158, 155,...]",

   "measures":"["sat":[...],"HR":[...]]"

   }

This step was **successfully validated**

2. Device formats and encrypts vitals data wholesale using hardened encryption library and base policy to be used by proxy service. Justification if not passed: failure in encrypting data, missing library, library related errors, missing policy.

This step was **successfully validated**

3. Device sends data to SADP which acts as a proxy service. Justification if not passed: failure to connect to proxy, malformed data, configuration issue.

This step was **successfully validated**

3.1. Proxy retrieves attribute key from key manager to decrypt data. Justification if not passed: unable to connect to key manager, failure to retrieve key, invalid key due to policy inconsistency.

This step was **successfully validated**

3.2. Proxy retrieves public key from key manager. Justification if not passed: unable to connect to key manager, failure to retrieve key

This step was **successfully validated**

4. Proxy retrieves hardened encryption policy from Telemed service according to patient ID reported in the data. Justification if not passed: failure to retrieve policy, connection error, invalid user ID, non-existent policy.

This step was **successfully validated**

5. Proxy encrypts the data with the given policy and key. Justification if not passed: error in the library, invalid policy or key.

   Example encrypted data

   {

   "timestamp":1679656096635,

   "session_type":"SPO2",

   "chart_patient":4,

   "chart_session":12,

   *"data": **ENCRYPTED**,*

   *"measures":**ENCRYPTED***

   }

This step was **successfully validated**

6. Proxy relays the encrypted data to the Telemed service. Justification if not passed: failure to connect to service, malformed data, connection error, configuration error.

This step was **successfully validated**

7. Telemed service stores encrypted data. Justification if not passed: malformed data, database failure.

This step was **successfully validated**

8. Remote Attestation of device considering the following actions:
    c. The Attester running in a smartphone was able to receive and process the remote attestation request/challenge, retrieving the selected (dummy) claims and nounce.
    d. The Attester was able to securely send - by invoking Hardened Encryption libraries - evidence (set of claims) to the Verifier.
    e. The Verifier was able to process the received response, confirming its nounce matches, and appraising the received Evidence against a simple policy (i.e., values match accepted or range of accepted reference values).

These steps have been **successfully validated**

6.3.2 Use-Case C3 - Personal data processing towards health alarm triggering

In the following we report on the validation of the health data processing use case, where the purpose of it is to detect health alarms by the MIoT monitoring tool. The ARCAIAN-IoT components participating in P1 validation are Self-Aware Data Privacy (SADP) and Hardened Encryption (HE).

The input into the use case is encrypted data originating from a patient's device (Use-Case C2). As reported in Section 6.2.9 the use of HE in C2 was successfully validated, hence it was possible to use such encrypted data and not just mock-ups. The following results were obtained:

1. The data processing Alert component deployed at the MIoT cloud service, with integrated Python HE library.
    a. Since integration with HE key management component is planned for P2, private cryptographic material was given to the Alert component without authorization.

This step was **successfully validated**

2. The Alert component requests encrypted data from the database.

This step was **successfully validated**

3. The Alert component uses the HE library and private cryptographic keys to decrypt the parts of the encrypted data that are needed for the data processing.
    - The decryption was successful obtaining the correct data and with minimal overhead. The SADP component used in C2 encrypted only parts of data that do not reveal the identity of a patient with a policy that the Alert component can access it. Parts of the data that do reveal the identity were decryptable by the Alert component.

This step was **successfully validated**

4. The result of the data processing is encrypted and forwarded to the SADP component, which decrypts it and further encrypts it with an appropriate access policy.
    - The alert component encrypted the data for the SADP and sent it to the database. The SADP component intercepted the call and decrypted the processing result. It retrieves

the appropriate access policies and re-encrypted the result with the refined policies.

This step was **successfully validated**

- The resulting encrypted is saved at the MIoT platform database.

This step was **successfully validated**

6.3.3 Use-Case C4 - *Monitor a patient and update a patient monitoring protocol*

Recalling this use case, it focuses on a Medical professional (Organization Member), being authenticated by ARCADIAN-IoT to access the MIoT hospital platform and manage patient records with integration to the following ARCADIAN-IoT components: (1) MFA; (2) hardware-based identification and authentication (network-based); and (3) the Self-Sovereign Identity (SSI) / Verifiable Credentials (VC) and (4) Self-Aware Data Privacy.

The following are all the foreseen steps of UC4, which were designed and partially validated in P1, delegating to P2 the final validations steps related to the interactions with users (medical professionals) and thus the Authentication and Identification components. This is due to the integration delays and partial availability of the needed components. On the other hand, thanks to the successful integration and validation of C2 and C3, data exchange in C4 (step 4 below) could already be validated with mocked-data and interfaces.

1. A medical professional access the MIoT hospital platform and chooses to be authenticated by ARCADIAN-IoT Framework (based on network eSIM token and SSI)

This step is **not validated.**

2. The medical professional is requested to open their mobile wallet before confirming to proceed to request their Organisation Verifiable Credential from the mobile wallet.

This step is **not validated.**

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.
    a. As part of this process the reputation of the medical professional is checked, and a low reputation could be a reason to deny access.

This step is **not validated.**

4. The medical professional accesses their patients´ dashboard to view any alerts or a specific patient´s data. The data that it receives comes from Use Cases C2 and C3 but in unencrypted form since integration with Hardened encryption and Self-aware data privacy is scheduled for P2.

This step is v**alidate**d because C2 and C3 are successfully tested and validated and will allow a faster uptake of C4.

5. Real-time requests for data can be made to the patient´s mobile app, such as a request to change the monitoring protocol. Authorization of these requests and encrypting the communicated data is scheduled for P2.

This step is **not validated.**

6. Medical professional login should be captured in MIoT hospital platform or SIEM.

This step is **not validated.**

7. The medical professional should be able to view patient data retrieved in real-time.

This step is **partially validated**. As in step 4 of the previous section, we have been able to validate that it works without the authentication part, which will be validated in P2.

8. The patient should be 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.

This step is **partially validated**. As in step 4 of the previous section, we have been able to validate that it works without the authentication part, which will be validated in P2.

9. When the reputation of the medical professional is reduced then it can be seen that an event is raised in the MIoT hospital platform and that the medical professional is denied access to the platform.

This step is **not validated.**

6.4 Evaluation Results - Currently Deployed Components

This section describes the KPI achievement of individual components upon their deployment on P1 use cases that are considered in this document.

6.4.1 Permissioned blockchain KPIs

Table 1 - KPI status for Permissioned Blockchain

Feature/Scope	Metrics	Target values	Evaluated value (P1)
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	1
deployment of permissioned blockchain in IoT environments	Number of peer nodes deployed	3	2

Following is a justification for the differences between the expected value and the value obtained for the KPIs:

- **Number of ARCADIAN-IoT services using permissioned blockchain =** "obtained 1”
  - Public sidetree DID is integrated with private Ethereum on preprod VM and meets this KPI.
  - The Permissioned Blockchain based on Hyperledger Fabric is recently deployed on preprod VM and is now ready for integration tests with HE & Reputation, but as yet no integration tests have started.

- **Number of peer nodes deployed =** "obtained 2”
  - Currently only 2 peer nodes have been deployed for initial integration tests.

6.4.2 Behaviour Monitoring KPIs

Table 2 - KPI status for Behaviour Monitoring

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Ability to process different input types with non-root privileges (syscalls, auth, rep)	Number of inputs considered	3	1
Deployment in heterogenous devices	Number of supported devices	2	1

The evaluation shown above was done using the integration of this component in the use cases B1 and B2. The evaluation is considered successful as it is as expected for this moment (P1).

With respect to the number of inputs considered, as it was mentioned before, we have verified that the behaviour monitoring component can be deployed on the Drone Hardware from Domain A (planned for P2), and it can be installed in a running container (as the Middleware from Domain B) and capture the container’s system calls. Nonetheless, even though integration with Domain B was planned for P1, only the authentication inputs were considered as it was not yet possible to conclude the set the middleware container to relay systems calls to the behaviour monitoring component.

6.4.3 Hardened Encryption (with eSIM) KPIs

Table 3 - KPI status for Hardened Encryption with eSIM

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Encryption library with fine access control	Number of API, number of types of platforms/devices demonstrated	>= 4, >= 2	3, 2
Efficient implementation of encryption/decryption	Computation time	Comparable to state of the art on multiple devices	achieved

- **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.

6.4.4 Hardened Encryption (with cryptochip) KPIs

Table 4 - KPI status for Hardened Encryption by cryptochip

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Provisioning time (for any scenario) into device side, with GUI in place and how to procedure, into device side. Provisioning time (for any scenario) with web dedicated page in place and how to procedure, into middleware side.	Operation time	<= 5 min <= 2 min	achieved
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.	Computation time	T1_E < 2s	T1_E is achieved
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	T4_D is in scope of P2 development
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	T3_E is in scope of P2 development
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	T2_D = 12s

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.

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).

6.4.5 Decentralized Identifiers KPIs

Table 5 - KPI status for Decentralized identifiers

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Support availability of decentralized identity management schemes	Support at least two of the use case domains	>=2	1
Support authentication for persons and IoT devices	Support "Persons· & "IoT Devices"	3	Persons

Following is a justification for the differences between the expected value and the value obtained for the KPIs:

- **Number of ARCADIAN-IoT pilot domains using Decentralized Identifiers =** "obtained 1"
    - Pairwise DIDs for SSI Wallets and public DIDs for the framework´s SSI Agent are now supported for use case domains A authentication. This is also available for integration with domain C, but is not actually scheduled for integration in P1 in domain C.
- **Support authentication for persons and IoT devices =** "obtained Persons"
    - Pairwise DIDs for SSI Wallets is supporting authentication in domain A. Support for IoT Devices is planned for P2.

6.4.6 Network-based authentication KPIs

Table 6 - KPI status for Network-based Authentication

Feature/Scope	Metrics	Target values	Evaluated value (P1)
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	1
	TRL	>=6	4/5

The evaluation shown above was done using the integration of this component in the use case A2 (section 3.2.2). The evaluation is considered successful as it is as expected for this moment (P1).

6.4.7 Biometrics KPIs

Table 7 - KPI status for Biometrics

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Low Inference Time for Face Verification Algorithm	Frames per Second (FPS) or Milliseconds (ms)	16 FPS / 62.5 milliseconds	16.5 FPS/ 60.6 ms
High Accuracy of the Face Verification Algorithm	mean Average Precision (mAP)	90% mAP	91.65% mAP
Reliable Recognition of the Face Verification Algorithm	False Acceptance Rate (FAR)	0.5% FAR	0.5 % FAR

Following is a justification for the differences between the expected value and the value obtained for the KPIs:

- **High Accuracy of the Face Verification Algorithm =** "91.05% mAP"

  The accuracy was extracted after evaluating the AI model with the testing dataset of AGEDB30. This dataset is considered as one of the most complex publicly available because it compiles a total of 16,488 images labelled with different identity, ages and gender attributes. There is a total of 568 different subjects with an average of 29 images per subject. Besides, the scientific community also present their accuracy results with LFW. In comparison with AGEDB30, LFW is a less complex dataset, therefore, the face verification algorithm reaches a peak of 99.41%.

6.4.8 Multi-factor Authentication KPIs

Table 8 - KPI status for Multi-factor Authentication

Feature/Scope	Metrics	Target values	Evaluated value (P1)
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	0
	Number of devices used simultaneously in a person's identification	2	1

The evaluation shown above was done using the integration of this component in the use case A2 (section 3.2.2). The evaluation is considered successful as it is as expected for this moment.

6.4.9 Verifiable Credentials KPIs

Table 9 - KPI status for Verifiable Credentials

Feature/Scope	Metrics	Target values	Evaluated value (P1)
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.

6.4.10 Remote Attestation KPIs

Table 10 - KPI status for Remote Attestation

Feature/Scope	Metrics	Target values	Evaluated value (P1)
Novel RATS-based Remote Attestation procedure	*Number of devices/OS platforms supported by remote attestation*	*2*	*1*
Attestation Results feeding both device and service reputation models	Types of IoT devices reputation affected by RA	1	0
Attestation Results feeding both device and service reputation models	Number of IoT services reputation affected by RA	1	0

Following is a justification for the differences between the expected value and the value obtained for the KPIs:

- *"Number of devices/OS platforms supported by remote attestation*": as planned RA has been validated for smartphones in the involved use cases (A3, C2), through smartphone. RA has also been successfully run on a Linux environment (Ubuntu OS), inside a docker container, which is the same used by the drone; however, considering that the package to run it specifically on the drone's environment is not done yet, we do not consider the drone environment/platform as validated at this stage.
- Types of IoT devices reputation affected by RA" and "Number of IoT services reputation affected by RA": both KPIs depend on the following features:
    - The ability for the Verifier to generate Attestation Results based on received Evidence: Currently the attestation results are generated based on dummy data, and the exact structure is open to adjustment (subject to the final interface with Reputation System).
    - The ability for the Reputation System to process / appraise Attestation Results (which may lead to updates in the Reputation of a Device): this is work in progress and will be supported in time for P2.

6.4.11 Reputation System KPIs

The reputation system KPIs are summarized in the following table. Some of the KPIs have been obtained in the Spark UI component that is integrated in the reputation system.

Table 11 - KPI status for Reputation System

Feature/Scope	**Metrics**	**Target values**	**Evaluated value (P1)**
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%

6.5 Overall Validation and Evaluation Deviations

This section compiles the most relevant validation and evaluation targets that were not completed successfully, and which have been documented in the Validation and Evaluation results (section 6). It is assumed that all the mentioned items will be addressed during P2 Validation and Evaluation and reported in the next D5.4 document version with the complete P2 results.

Use Case A3 was partially validated in P1 with the following deviations:

- **Reputation System (RS)**
  - The reputation values are used to authorize the personal device to access to the network, and consequently to exchange data with the DGA service. Also, to authorize the access to the network according to the reputation values and reputation policies. These results have been partially achieved with three types of policies (as described before). However, it was yet not validated the use of reputation information from the DGA service.
- **Hardened Encryption (HE)**
  - This is not a formal deviation but rather a consequence of development planning as HE integration was set for P2.

Use Case C4 was partially validated in P1:

As explained in Deliverable 5.3 (Section 4.4.3) it was possible to implement a functional Use Case C4. However, it was not possible to perform a complete C4 Use Case validation within P1 for the following reasons:

- **Use Case C4 has changed** from what was defined in WP2 so that a Medical Professional would now be authenticated by the ARCADIAN-IoT instead of its own MIoT Application.
- Use Case C4 would then **depend upon a pre-requisite** from Use case C1, which have a planned delivery and validation for P2.

7 PROGRESS TOWARDS ACHIEVING PROJECT OBJECTIVES AND KPIS

This section recaps the project-wide Objectives and related KPIs, and describes the associated contributions and achievements so far (i.e., at the moment of P1 validation).

7.1 Objective #1

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

Main Achievements:

ARCARDIAN-IoT implements a decentralized framework that exposes security services for IoT systems validated by a set of Use-Cases in the context of Domain A, B and C. The core aspect of decentralization - and the associated resilience against attacks - is intrinsic to the progress observed in multiple of its functionalities across different planes. Within the Identity management plane, the **Decentralized Identifiers** provides the different end user stakeholder organisations, their own means to cryptographically prove that their services, end users, members and IoT Devices are the holders of certain credentials.

In the Trust management plane, the **Verifiable Credentials** provides for various actors to act as issuers of credential e.g., simulator of national bodies for issuing national eID person credentials and organisations to issue their members/employees with credentials as well as IoT Devices. This creates a decentralized self-sovereign Identity approach in the ecosystem.

As for the Common plane, the **Permissioned Blockchain** further enables distributed / decentralized storage for publishing information across the planes and available to external parties in the ecosystem (e.g., Security management plane, with **Hardened Encryption** publishing cryptographic key information). Currently the Publisher Smart Contract is deployed on 2 peer nodes in pre-production for integration tests. In Addition, the **Reputation System**, also part of the Trust management plane, allows to determine the reputation of heterogeneous entities, and work has been initiated to store the reputation values in a decentralized fashion, by defining the required smart contracts and the mechanisms to store reputation values in the **Permissioned Blockchain**.

7.2 Objective #2

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

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

Main Achievements:

The work performed to achieve this objective included the research performed for supporting the different IoT object identification methods. From the one hand, aiming at chaining **Decentralized Identifiers** and **Verifiable Credentials** identification methods with the Self-Sovereign Identity

approach, in the reported period the following progresses should be highlighted: a) the decision for the **Decentralized Identifiers** exploiting the Sidetree specification from the Decentralized Identity Foundation (DIF) and leverage the **Permissioned Blockchain** as trust anchor for published Decentralized Identifier Documents (in a notarization approach); b) the decision for implementing the **Verifiable Credentials** based on Hyperledger ARIES GO framework provided by the ATOS SSI solution Ledger uSelf, which is extended to support persons (contributing to O3), and organisation issuer IdP and support of more restricted deployments on IoT devices as well as researching additional protocol support and cryptographic signing algorithms.

Regarding **eSIM**[6], the progresses have been multi-fold, and reflect the enforcement of its role in the project context beyond a hardware-based identification mechanism, supporting also processes such as device self-protection and recovery; moreover; the novel **multi-factor authentication** approach for devices, exploiting the combination of eSIM and SSI functionalities for increased identification robustness against attacks (e.g., impersonation) has been implemented and integrated. Strategically, TRU, ATOS and UWS chose to research, develop and validate ARCADIAN-IoT's persons identification (O3) first (in an MFA approach). The reasons that support this decision are that (1) it allowed all partners involved in identification mechanisms to start integrating their work (including the UWS, who focus on biometrics, component that don't participate in objects' identification); and (2) having the persons' authentication consolidated, the devices' authentication operation is similar, having most of the challenges overcome (just the public decentralized identifiers and the hardware-based identification applies to objects). Therefore, focusing on eSIM component use on identification, while at the moment it was not formally validated for device identification, considering that it was validated for person identification (through the person personal device), no major challenges are expected to validate it with any IoT device because the eSIM-based identification in agnostic to the cellular device (as long as it is following standards). Therefore, in what regards eSIM, no demanding challenges are expected to fulfil the KPI2.1 and the KPI2.3. In what regards KPI2.2, the eSIM is acting as Root of Trust able of providing digital signatures, by using unique secrets generated in the hardware secure element of each device. This decentralized approach that allows to identify the data producers based on RoT information attached to the data has been validated in lab for IoT devices, being now ongoing its research and development for Android devices for fully supporting the targeted use cases.

7.3 Objective #3

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.**

Main Achievements:

[6] ARCADIAN-IoT's Subscriber Identity Module (SIM) technologies are agnostic to the form factor, being applicable to at least SIM, eSIM and iSIM

The novel **Multi-Factor Authentication**(MFA) approach for persons, combining 3 multiple simultaneous identification forms, specifically the(eSIM-based) network identifiers, biometrics and SSI has been implemented, integrated with a IoT solution and validated in lab environment for that domain– see3.2.2 and 6.1.2. Therefore, the KPI3.4 is in a good track to be considered accomplished.

Regarding the decentralized SSI approach for identifying persons in a privacy-compliant way, the research on the **Decentralized Identifiers** specification resulted in the decision to exploit the Sidetree specification from the DIF and leveraging the **Permissioned Blockchain** as trust anchor for published Decentralized Identifier Documents (in a notarization approach); moreover, the research on the **Verifiable Credentials** has enabled to reach the decision to use Hyperledger ARIES Framework ,making use of the ATOS SSI solution Ledger uSelf as baseline, which will be extended throughout the project to provide additional functional support and cryptographic signing algorithms. In order to fulfil KPI3.2, a plan has been established in deliverable “D5.6 – Training and Security and Privacy Awareness activities report”.

Towards further ensuring the Identity management approaches compliance with GDPR pair-wise peer DIDs are used in the SSI Wallet, and to promote privacy for IoT Devices leveraging **Permissioned Blockchain** as anchor trust for public DIDs, the cryptographic key information is stored off-chain. 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 recognition with the Biometrics component has focused on the face verification in 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 0.5% - which enables the fulfilment of KPI3.1.

In meeting KPI 3.3, ARCADIAN-IoT issues person eIDs following the specification of EBSI natural person schema[7] that is aligned with the eIDAS minimum data set. This aims 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[8].

7.4 Objective #4

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).

Main Achievements:

7 https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+ID+-+Natural+Person

8 https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

To contribute to this objective, the specification and implementation of the individual elements of the Chain of Trust have been progressing. Regarding the distributed trust/ **Reputation System**, for building reputation of a given entity (e.g., person, device or service/app) according to the information retrieved from events. At the time of writing this deliverable, two models for reputation have been designed and partially implemented. The Alpha-beta (documented in D2.4) and the prioritized Alpha-Beta models are applicable to all the type of entities. The model with priorities allows to distinct events that can reset the value of the reputation or that include severity information that can impact the reputation score. As stated for O1, the work towards storing reputation scores in a **Permissioned Blockchain** has been initiated with the design of smart-contracts and technological choices (using Hyperledger Fabric). The **Network-based Authorization** has been specified to enforce security policies in the cellular network core (between devices and the internet) according to trust information provided by the Reputation System. A first prototype with simple policies has been implemented and validated in a local machine with emulated IoT devices using an open-source network core testbed (Open5GS). This testbed is already deployed and integrated with TRU's production cellular networks to be able to integrate the component with IoT solution providers' devices and demonstrate it. Having the final set of rules agreed with the Reputation System (UC), the current research efforts are in implementing these rules programmatically in the network core. This component will confirm the availability of trust evaluation models for heterogeneous entities (KPI4.4) using it for protection of data and of vulnerable devices.

With respect to the **Federated AI**, 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. In addition, Federated AI is also employed in ARCADIAN-IoT components such as the **Device Behaviour Monitoring**. This achievement contributes towards addressing the KPI 4.1. Besides of data rebalancing models, 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. For IoT device intrusion detection capabilities of **Behaviour Monitoring**, the training of models has been performed, as well as initial evaluation activities comparing against considered baseline results. The Device Behaviour Monitoring component has also fulfilled KPI 4.3 as its ML models can now detect anomalous behaviours with an accuracy of approximately 96%.

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.

Finally, a first version of 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), as well as validated in smartphone devices (Android OS). The attestation results (or outcomes) will provide the **Reputation System** with valuable trust indicators regarding the IoT devices, contributing to the Chain of Trust.

7.5 Objective #5

Objective 5: Provide a hardened encryption with recovery ability.

- **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.

Main Achievements:

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 eUICC / **eSIM** as secure element has been validated in lab in IoT 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. API for JavaScript are currently being 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. It has been internally tested and is currently being validated in Use case C. The main effort that is currently in progress is to decentralize the key management component and integrate it with ARCADIAN IoT Multi-Factor Authentication and Permissioned blockchain.

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 both Domain B (grid) 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).

Regarding **eSIM** as hardware-based RoT for hardened encryption, the previously specified approach, it is using GSMA IoT SAFE specification as baseline. The approach consists of using the eSIM RoT for signing data encrypted in the device with the ABE. The first prototype, focusing IoT devices, has been integrated with the Hardened Encryption ABE libraries, enabling strengthened encryption for avoiding, for instance, impersonation attacks. The research on applying this technology on personal devices is ongoing. The use of eSIM as RoT is on track for fulfilling KPI5.2.

The integration of Hardened Encryption (as an horizontal feature from the Common plane) with

the Trust Management Plane has progressed as mentioned, being used for encrypting and thus ensuring confidentiality of the attestation evidence and enabling selective decryption (i.e., only a determined Verifier is able to decrypt and appraise a given evidence); the integration of the Hardened Encryption with the Identity plane is currently in progress,, with the **Biometrics** component encrypting private photos of users for data protection.

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.

7.6 Objective #6

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.

Main Achievements:

The work for fulfilling this objective during the project duration includes: 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 **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 second being the recovery of data and services - both being 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., a device with compromised security will inform the device application which will decide on the need to go through the process of **Credentials Recovery**). Credential Recovery design has been agreed and will be proven for P2 – i.e., no integration took place in P1. The contributions mentioned in previous Objectives regarding the **Device Behavior Monitoring** (aiming at 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** cooperation with Self-Recovery is aimed at enabling KPI6.1 – the achievable recovery degree is yet to quantify at this point in time and is subject to be established according to the incident-related use cases to be validated in P2.

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.

7.7 Objective #7

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).

Main Achievements:

The work performed on the **Cyber Threat Intelligence (CTI)** during Y2 consist of: (i) setup of MISP in RISE's Cyber Range, (ii) implementation of extensions for the MISP-based engine (e.g., automatic event/attribute fetching), (iii) definition of the tinySTIX data format and corresponding communication models for IoT systems, (iv)definition of a feature set to be deployed by CTI's machine learning models, (v) design, and preliminary implementation of three machine learning models for the threat level ranking, federated event classification, and smart IoC sharing; Finally, as for the collection by the **CTI** of 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 **Behaviour Monitoring**). These efforts, and the work on **Federated AI** on a new data rebalancing model for privacy-preserving federated AI (described as part of Objective 4 / Section 7.4), directly address KPI 7.2.

As of P1, the **Behaviour Monitoring** is not yet issuing Indicators of Compromise as it was not part of the planned activities. Nevertheless, the specification of the messages and alignment of the protocol's specificities (e.g., STIX and TAXII) have already been discussed and will be implemented during P2 development. The described activity mainly considered issuing of IoC's by the Behaviour Monitoring. However, partners have also initiated discussions with respect to the consumption of IoCs - in this case, consumption of IoCs by the **Device Self-Protection** component to trigger the enforcement of IoT device self-protection policies, and for the IoT device trust/reputation updates (used by the **Reputation System**). The work to consider IoCs for the determination of reputation has been initiated. These activities are mostly related to KPI 7.1.

8 CONCLUSIONS

This document reports the validation and evaluation effort, focused on the first prototype (P1) of ARCADIAN-IoT Framework with available Use-Cases and KPIs, and being part of Task 5.5, due on M24 of the project. The validation and evaluation followed the components and Use-Case integration activity and availability during T5.1 execution (Integration activity) and T5.2, T5.3 and T5.4 definitions (for the Use-Cases detailed definition and preparation).
All partners were involved in the validation and evaluation activities using the ARCADIAN-IoT framework in the context of the 3 domains identified by the project.

In this document, the adopted validation and evaluation approach, scope and methodology were presented in the initial sections. The deliverable presented three main validation and evaluation aspects: (1) the technical validation of the Use-cases; (2) the technical evaluation of the project/components KPIs; (3) the legal validation. It was also provided a description of the current ARCADIAN-IoT validation and evaluation results according to the P1 scope identified.
Overall, the 8 Use-Cases identified for P1 and related 14th component associated KPIs used for validation and evaluation, despite some minor deviations descripted in the previous sections, were successfully validated and KPIs measures obtained accordingly to what was expected.

It is expected that the validation and evaluation will continue for the second planned prototype (P2), onboarding the remaining Use-Cases and KPIs, as well as the points expected to be in the scope of P1, but that for some reason could not be completed in the time of P1 validation and evaluation milestone.

REFERENCES

[1] ARCADIAN-IoT, “D5.1 - Integration of ARCADIAN-IoT framework,” 2022.

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

[3] ARCADIAN-IoT, “D3.1 - Horizontal Planes - first version,” 2'22.

[4] ARCADIAN-IoT, “D4.1 - Vertical plane of ARCADIAN-IoT – First version,” 2022.

[5] J. Z. E. M. S. a. M. I. X. Wang, “Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT,,” in *International Conference on Communications (ICC)*, Sydney, NSW, Australia, 2014.