Grant Agreement N°: 101020259

Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D2.4: ARCADIAN-IoT framework requirements

Revision: v.2.0

Work package	WP 2
Task	Task 2.2
Due date	31/12/2021
Submission date	30/12/2021
Deliverable lead	LOAD
Version	2.0

Abstract

This report constitutes the deliverable D2.2 of ARCADIAN-IoT, a Horizon2020 project with the **grant agreement number** 101020259, under the topic **SU-DS02-2020**, and has the purpose of detailing the requirements for each component of the ARCADIAN-IoT framework.

Keywords: ARCADIAN-IoT requirements; IoT solutions specification; project validation; legal, ethical, regulatory and social dimensions

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	10/12/2021	First draft	LOAD (lead), All
V2.0	30/12/2021	Refinement with internal review feedback	LOAD, ATOS, Security Advisory Board

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

This report represents delivery D2.4, being an outcome of Task T2.2, which aims to gather the requirements that will inform the research to be performed in WP3 and WP4, and that will also facilitate the assessment of the project iteratively in WP5.

An analysis shall be done regarding distributed, dynamic and automated trust management and recovery solutions; also, approaches to manage the identity of persons and objects, including self-encryption/decryption schemes with recovery ability will be explored.

This study will be combined with the outcomes of Task 2.1, towards the definition of the technical requirements for the framework.

The output of the initial version of this report will be used for the architecture specification in Task 2.3, launching the work of WP3 and WP4 and defining the evaluation KPIs.

Following on from this deliverable, an agile approach will be taken for followed for the architecture definition and implementation of all the ARCADIAN-IoT framework components, which can lead to adjustments, changes and/or improvements to the requirements, while the architecture is being defined and work is ongoing, until the end of the project.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AB	Advisory Board
AGA	Annotated Model Grant Agreement
CA	Consortium Agreement
CFS	Certificate on the Finance Statement
CO	Project Coordination
DID	Decentralized Identifiers
DoA	Description of the action
EB	Ethics Board
EC	European Commission
ECAS	European Commission Authentication Service
EU	The European Union
FSIGN	Financial signatory
GA	Grant Agreement
PC	Project Coordinator
PFSIGN	Project Financial Signatory
PO	Project Officer from the European Commission
PM	Project Manager
RIA	Research and Innovation Action
SAB	Security Advisory Board
SC	Steering Committee
TC	Technical Coordinator
TCo	Technical Committee
WP	Work Package

1 INTRODUCTION

The ARCADIAN-IoT framework relies upon a novel approach to manage, in an integrated way, identity, trust, privacy, security and recovery. Orthogonal planes are combined in an optimized way to support the end-to-end services. The full chain of services/components, starting on the persons interacting/owning the IoT devices, which have the ability to collect and send data towards applications/services located at the edge/cloud network side processing the collected data.

The ARCADIAN-IoT framework includes vertical planes devoted to identity trust and recovery management, which are supported by horizontal planes managing privacy of data, security of components and decentralized storage through blockchain technologies, as illustrated in Figure 1.

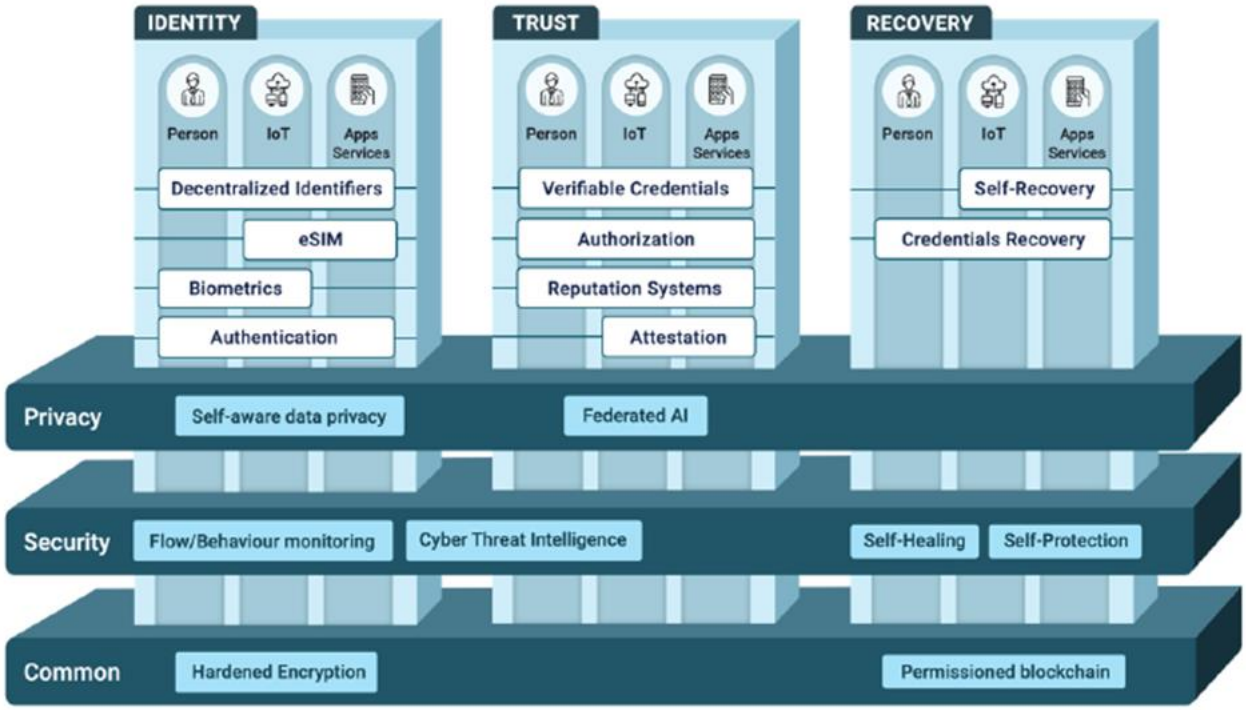

Figure 1 - The ARCADIAN-IoT framework

The ARCADIAN-IoT framework is evaluated in three realistic IoT domains: A) Vigilance and emergency in smart cities; B) Grid infrastructures; and C) Medical IoT.

The ARCADIAN-IoT concept towards a holistic framework - ARCADIAN-IoT Framework - chains multiple planes to manage different types of entities, namely persons, interacting with IoT systems, devices collecting data and Apps/services processing the collected data.

2 RESEARCH METHODOLOGY

The nature and complexity of the challenges in hand require an effort of co-creation joining academia, industry, IoT domain/solution experts, end-users, and cybersecurity specialists. The ARCADIAN-IoT consortium has a diverse set of partners that allows to join the different perspectives needed towards the holistic framework targeted.

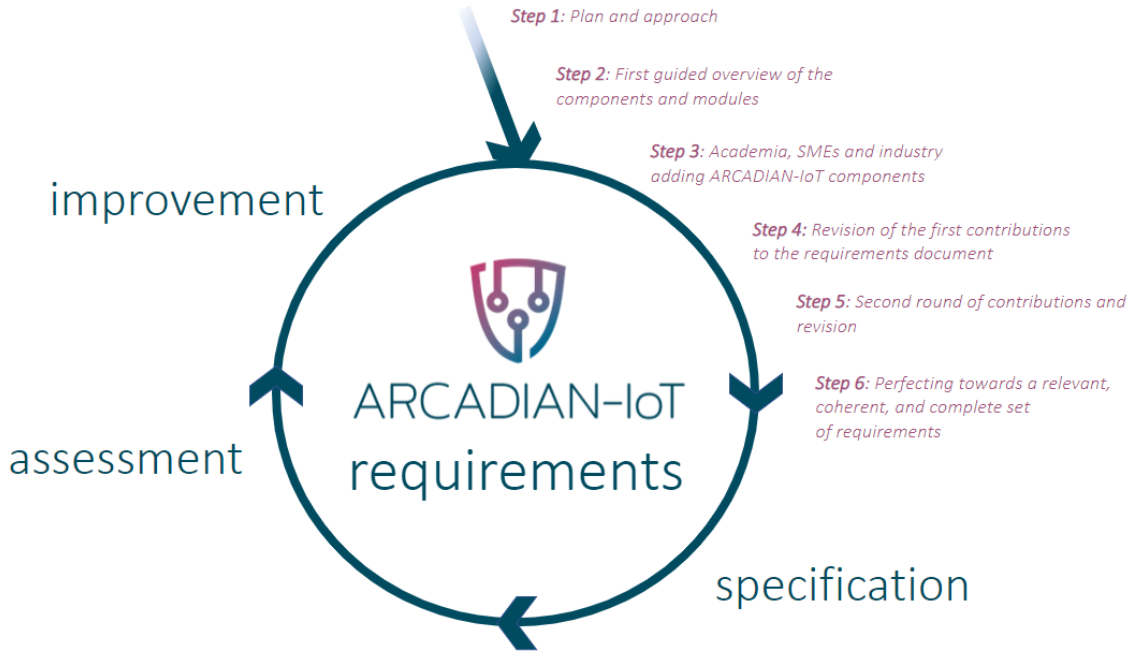

Figure 2 - Task 2.2 research methodology

Having in mind the co-creation needs and the problem complexity, the research methodology used in task 2.2 has an iterative nature, aiming for cyclically specifying, assessing and improving the use case set. The following steps describe the research methodology and techniques used.

Step 1: Plan and approach

The first step in task 2.2 was the definition of the plan and approach to fulfil the task objectives. Despite the iterative/agile approach, the task had a strict timeframe that needed to be considered to define the stages needed to accomplish the task goals. These stages are the steps described in this section. As can be seen in Figure 2, steps 1 and 2 are part of the research cycle, and other ones enter in iterations that can be described as of being of assessment of the previous step results, definition of the improvement needed in that step, and the enhanced specification of the use cases.

Step 2: First guided overview of the components and modules

The second step of the research process, was to attend jointly with T2.1 team to a set of workshops about the challenges and use-cases of T2.1, facilitated by its task leader but led by the IoT domain/solution experts and end-users of the consortium.

At this point, the component specification fields started to be defined, in order to prepare each component description, state of the art, requirements and expected outcomes.

Step 3: Academia, SMEs and industry adding ARCADIAN-IoT components

Basing on the horizontal and vertical planes identified for the component's architecture, and also on the information structures specified on Step 2, the partners experts in the components of ARCADIAN-IoT framework, started providing inputs and comments to each component's Description and State of the Art sections. This contribution was being done while T2.1 was in course, taking advantage of a better definition of the component's interaction after its usage in each of the use-cases of the 3 domains.

Step 4: Revision of the first contributions to the requirements document

A first revision of the document was done, identifying the missing fields and components that were not being filled. A specific workshop was done to clarify the doubts of come partners regarding what to fill and where. Task 2.2 leader gathered all the missing content and the partner responsible for it, and made individual requests with a list of missing contributions.

Step 5: Second round of contributions and revision

A second round of contributions to the document was initiated, now focusing on the specific requirements for each component and also its expected achievements (or KPIS). A new revision was done, focusing on giving overall consistency to the requirements. Some missing spots were still identified and a second round of follow-up collaboration was done with the involved partners asking them specific pieces of content still needed.

Step 6: Perfecting towards a relevant, coherent, and complete set of requirements

Finally, based on all the workshops with all participants of task 2.2, the last step consisted of perfecting the deliverable towards a coherent, meaningful and, completeness, and coherence. As result, the identified requirements, their applicability to the use-cases of T2.1 and their interaction reflected in the preconditions and postconditions will now consist of a major contribution to the architecture definition, being done in T2.3.

3 REQUIREMENTS

3.1 GENERAL REQUIREMENTS

3.1.1 Entities compliance with ARCADIAN-IoT

3.1.1.1 Persons

A compliant ARCADIAN-IoT person/user:

- Has at least 3 multiple simultaneous identification mechanisms: Self-Sovereign Identity (SSI) [Verifiable Credentials (VC), Decentralized Identifiers (DID), eIDAS regulation, …], identifiers related with his/her personal device (e.g., network credentials), and/or biometrics.
- The SSI approach in ARCADIAN-IoT aims to be compatible with European Self-Sovereign Identity Framework (ESSIF) and the eIDAS identity schemas.
- In the interaction with ARCADIAN-IoT services, accepts the Terms of Service related with the eSIM/RoT, Behaviour/Flow monitoring, Self-aware data privacy, Reputation, Attestation, Federated AI, Authorization, Authentication, and all the components where the person entity participates, or his/her data is collected/transported.

3.1.1.2 IoT Devices

A compliant ARCADIAN-IoT device:

- Has an embedded RoT hardware, particularly an eUICC/eSIM or a cryptochip, that securely provides identification and encryption material to the device.
- Has procedures in place (in an app or firmware) for being integrated in ARCADIAN-IoT framework and with all the components where the IoT device participates.

3.1.1.3 Services/Apps

A compliant ARCADIAN-IoT service or app:

- Has procedures in place (e.g., implements processes and exposes APIs) for being integrated in the ARCADIAN-IoT framework and with all the components where the service/app participates.

3.2 IDENTITY Vertical Layer

3.2.1 Decentralized identifiers

3.2.1.1 Summary

ARCADIAN-IoT will provide identity management based on W3C Decentralized identity specification [2] to enable identification of entities, human and non-human.

3.2.1.2 State of the Art

Decentralized Identity Foundation[1] (DIF) is a non-profit organization that aims to “Enable a world where decentralized identity solutions allow entities to gain control over their identities and allow

[1] https://identity.foundation/

trusted interactions".

DIF members are among the main contributors to W3C standards for SSI, with several working groups for DID related topics of special interest within ARCADIAN-IoT:

- Identifiers and Discovery[2]: protocols and implementations that enable creation, resolution, and discovery of decentralized identifiers and names across decentralized systems.
- DID Authentication[3]: Design, recommend and implement authentication and authorization protocols that rely upon open standards and cryptographic protocols using DIDs and DID Documents.
- DID Communication[4]: Produce specs for secure, private and authenticated message-based communication, where trust is rooted in DIDs and depends on the messages themselves.

The Members of DIF work to develop specifications and standards to be used as implementation reference, provide open-source implementations of the technical components and protocols they create and promote coordination among industrial organizations in de Decentralized Identity space. One of this specification is the Decentralized Identifier Core Architecture, Data Model and Representations [5], with a latest version released in August 2021, where DID is described as: "A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically".

A DID is a URI composed of three parts; scheme identifier, a DID method and a specific identifier within the DID method. Examples can be found in the W3.org website[6].

DID URIs resolve to DID Documents that contain information associated to a DID. They contain verifications methods (cryptographic public keys), and services to interact with the subject of the DID. ARCADIAN-IoT DID solution will follow the basic architecture model as described in the specification:

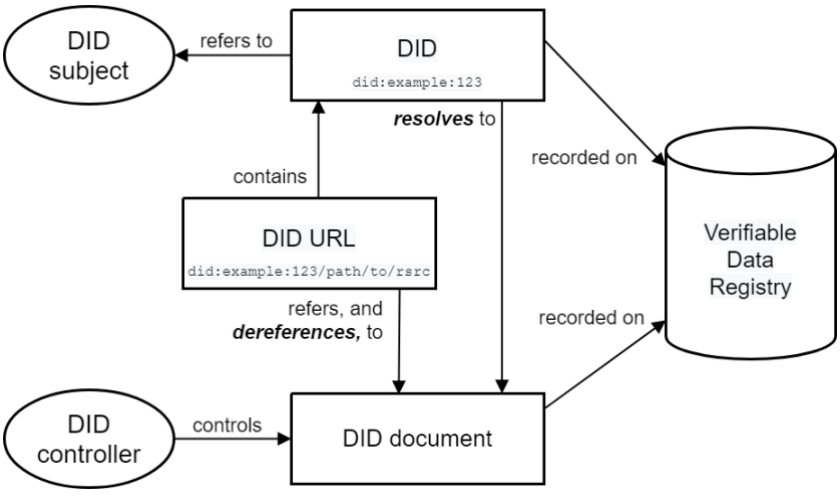

Figure 3 - Arcadian-IOT DID solution's basic architecture model

[2] https://identity.foundation/working-groups/identifiers-discovery.html
[3] https://identity.foundation/working-groups/authentication.html
[4] https://identity.foundation/working-groups/did-comm.html
[5] https://www.w3.org/TR/did-core/
[6] https://www.w3.org/TR/did-core/diagrams/parts-of-a-did.svg

DID method is an implementation of the features described in the DID specifications, to answer specific needs usually related to verifiable data registry. It specifies the operations by which DIDs and DID documents are created, resolved, updated and deactivated. DID method specification is defined looking for the interoperability between different implementations of the same DID method. Some of the are specifically targeted the IoT ecosystem:

- Tangle DID[7]: It is the DID method implemented by IOTA foundation[8] for their open-source distributed ledger, which is designed for the IoT ecosystem. It is a feeless ledger aimed to enable transactions between human and things.
- IoTeX DID: it is another DID method implemented for the IoTeX network. It is a Blockchain system designed for the exchange of value within the IoT ecosystem.

In the latest dates some initiatives to unlink DID from blockchain technologies are taking momentum to overcome their limitations and avoid, in some cases, extra costs. To this end new DID methods are being proposed:

- Peer DID[9], aimed to provide a solution for scenarios of private relationships between people, organizations and things. This DID method has no transaction costs. It is not persistent in any central system. Only parties participating in a relationship know the DIDs involved. It is interoperable with other Blockchain based DID systems.
- DID key[10]: it is a DID *Blockchainless* implementation to be used for a single, ephemeral interaction which do not need to be registered, updated, or deactivated.
- DID ORB[11]: self-certified DIDs that can be propagated without the need of the reliance provided by Blockchain technology. Instead, it uses a decentralized federation mechanism
- DID WEB[12]: it uses existing reputation of web domains in conjunction with blockchain based DIDs to provide meaningful trusted information about identities.

[7] https://github.com/TangleID/TangleID/blob/develop/did-method-spec.md
[8] https://www.iota.org/
[9] https://identity.foundation/peer-did-method-spec/index.html
[10] https://w3c-ccg.github.io/did-method-key/
[11] https://trustbloc.github.io/did-method-orb/
[12] https://w3c-ccg.github.io/did-method-web/

3.2.1.3 Requirements

Requirement 1.1.1 – Decentralized Identity Management
Description: To provide Decentralized Identity Management to enable secure and authenticated identity and other claims needed by the services and apps in the IoT ecosystems
Related to Use Case Domain / Category / ID / Name
(Use Case Domain / Category / ID / Name) *A1, A2, A7* *Desirable: B1, B3, B4, B6* *C1, C2, C4, C5, C7, C*
Requirements Scope (Person/IoT/Apps Services)
(*Personal devices IoT devices)*
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.2.1.4 Evaluation KPIs

1) Number of issued DIDs.
2) Number of verification methods.
3) Number of verification relationships.
4) Number of DID successful verification.
5) Number of DID failed verification.

3.2.2 eSIM

3.2.2.1 Summary

In ARCADIAN-IoT, we aim to leverage the potential of the latest SIM technologies to provide secure hardware-based identification of M2M devices and persons, not only in the context of cellular networks but extending it to all the relevant IoT third-party services, like Cloud or P2P infrastructures. eSIM/eUICC will also be used as a RoT for securely storing cryptographic material for hardened encryption in the IoT devices and, with its secure and independent communication over-the-air with network core elements, perform actions that reduce the impact of attacks of compromised devices.

3.2.2.2 State of the Art

Despite advancements in cellular technology, most IoT devices still rely on Wi-Fi connectivity[13]. Wi-Fi provides great coverage in a very limited area. Building IoT on limited connectivity restricts the scope. Although Wi-Fi provides some comfort, current deployments are performed in an isolated fashion, with their own network managers and with non-scalable security policies (e.g., impracticable to regularly update Wi-Fi password when the number of devices can scale to the order of 10 billion). Mobile IoT is undeniably the next frontier in the secure connected devices market. Network technologies such as 5G, NB-IoT and LTE-M are being rapidly deployed and simpler solutions for securely distributing and activating IoT devices with mobile connectivity are now available. Devices (for connected homes, monitoring pollution, etc.) are being created to be network agnostic and connect out-of-the-box wherever they are. This is where eSIM shows its strong value[14].

SIM technologies are well accepted as secure enablers for devices/subscribers' identification in mobile networks. Traditional SIM (physical) cards are safeguarded by using secure facilities for manufacturing which includes all the secure elements and data needed in order to establish a session. The eSIM extends the reach of these secure facilities to anywhere where there is an internet connection, using protocols that enable the secure exchange of data. The SIM can be applied in two contexts:

- Consumer (mobile), that is used directly by the consumer and needs consumer interaction and authorization.
- Machine to Machine (M2M), where the focus is business to business, specifically IoT markets.

The latest eSIM technologies add digital, over-the-air management, to the older SIM processes, avoiding end user interaction and enhancing the scalability of the process, while maintaining its security.

This Remote SIM Provisioning novelty for M2M is composed of 3 elements[15]. The SM-DP (Subscription Manager - Data Preparation) prepares, stores, and protects profiles (including the operator credentials). The SM-SR (Subscription Manager - Secure Routing) secures the communications link between the eUICC and SM-DP. The eUICC is the hardware-based secure element present on the device that contains one or more profiles - each of which contains all the elements needed to identify the subscriber in the networks. In the M2M solution, the mobile device normally operates without any local human control of connectivity (push model).

---

[13] https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/
[14] Truphone and Synopsis, “Securing the Mobile IoT White Paper” 2019.
[15] https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

For the consumers solution, the base was the M2M solution but with more complex use cases and requirements related to end-user managed devices, i.e., considering the end user interaction via the interface available. The SM-DP+ is a new component, which integrates the features and responsibilities of SM-DP and SM-SR in the M2M solution. There is an LPA (Local Profile Assistant) that consists of a set of functions for downloading the encrypted profiles to the eUICC and manage those profiles. The SM-DS (Subscription Manager - Discovery Server) provides a means for an SM-DP+ to reach the eUICC without having to know which network the device is connected to. Contrary to the M2M solution, the consumer approach requires that all subscription profile operations are under end user control, or at least subject to end user permission (pull model), as illustrated in Figure 4:

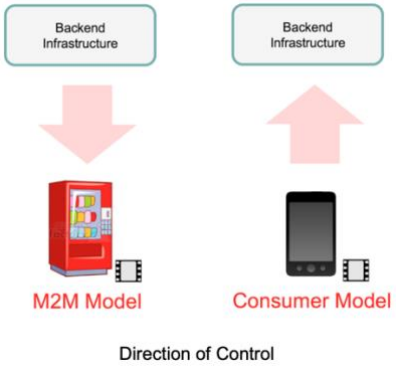

Figure 4 - Direction of Control of the two models

Both architectures are GSMA-defined[16] [17] but it should be noted that although there are architectural similarities between the Consumer and M2M solutions, they are inherently technically different and cannot be overlapped in an implementation that serves both Consumer and M2M2. The specifications also define the various interfaces between the components mentioned, including Over-The-Air (OTA) interfaces for Operator-eUICC communication (ES6) and profile download and installation interfaces between the SP-DP/SP-DP+ and the UICC (ES8/ES8+)[16] [17]. These OTA communications can use SMS, CAT_TP and HTTPS for their communication with the eUICC[17].

In the consumer solution, where the pull model is used, it is common to have an application capable of interacting with the eUICC. The Android operating system requires that such application possesses Carrier Privileges, i.e., the application shall be signed with certificates stored in the UICC itself[18]. With those privileges in place, the application and its developers can use special APIs to communicate with the eSIM and the eUICC, all according to the interfaces established by GSMA[19].

More recently, work has begun in a new IoT specification directed at network constrained devices and/or UI constrained devices. This new set of requirements aims to facilitate the remote provisioning (download, enable, disable, delete) of eSIM profiles in multiple scenarios, where connection-oriented protocols (e.g., TCP/IP) or text messaging (SMS) may not be available. The architecture should support lightweight protocols (e.g., CoAP) to ensure the transfer and download of the profiles to the devices.

Another concern of this specification is the intermittent nature of the IoT device lifecycle. Any management operation should aim to be performed asynchronously, whenever the device

[16] https://www.gsma.com/esim/wp-content/uploads/2021/07/SGP.21-2.3.pdf
[17] https://www.gsma.com/esim/wp-content/uploads/2020/07/SGP.02-v4.2.pdf
[18] https://source.android.com/devices/tech/config/uicc
[19] https://source.android.com/devices/tech/connect/esim-overview#EuiccCardManager

connects itself. Also, due to battery savings and the expected extended lifetime of the devices, traffic, number of operations in disk, size of the payloads, among other factors, should be optimized and taken into account.

An interface for factory provisioning of the profiles is being discussed and could be a way to ensure one less remote operation between the IoT devices and the management system.

Some components that exist in the Consumer specification are leveraged in the new IoT specification, like the SM-DP+ and the SM-DS, but a new eSIM IoT remote Manager (eIM), responsible for the remote profile management operations, and a new IoT Profile Assistant (IPA), that provides functions that enable the eUICC to be provisioned via SM-DP+, are introduced. It is worth noting that an eSIM may manage more than one device, with no need to exist a one-to-one relationship between the components. In the same way, an IoT device may have more than one manager and may store the manager's public key to authenticate the operations received.

(This specification is still a work in progress and GSMA's goal is to do a public release in late 2021/early 2022. As such, some of this information may be subject to changes.)

GSMAs eSIM ecosystem[20]

The current M2M and consumer solutions require the verification of:
● **eUICC Security**, referencing a Common Criteria Protection Profile[21] [22] to the assurance level of EAL4+, with the consumer solution focusing only (so far) on a silicon-level Protection Profile (PP0084)[23];
● **Production Environment and Process Security**, via the GSMA's Security Accreditation Scheme[24];
● **Functional Compliance**, for M2M based on the GSMA's test specification[25]. GlobalPlatform have created and run a functional test and qualification programme for eUICCs based on the GSMA defined test cases. For the consumer solutions, functional test and certification programmes based on GSMA test specification SGP.23. These programmes have been established, in partnership with GSMA, by GlobalPlatform (for eUICC), Global Certification Forum[26] and PTCRB[27].

It is worth mentioning that only eUICC manufacturers, SM-SR and SM-DP hosting organisations (for M2M) and SM-DP+ and SM-DS (for the consumer solution) hosting organisations that have successfully proven their compliance to both the security and functional requirements can apply for the necessary certificates from the GSMA Certificate Issuer to participate in the GSMA approved M2M and Consumer solution ecosystem. This is the case of *TRU* that holds GSMA Security Accreditation Scheme certification. In ARCADIAN-IoT, we aim at extending eSIM ecosystem technologies, keeping at least the same level of security, to provide secure authentication of M2M devices and mobile consumers to all the relevant IoT third-party services.

IoT SAFE[15], defines how to use the eSIM as a Root-of-Trust, opening the way for the extension

---

[20] https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf
[21] https://www.commoncriteriaportal.org/
[22] https://www.gsma.com/newsroom/wp-content/uploads/SGP_05_v1_1.pdf
[23] https://www.commoncriteriaportal.org/files/ppfiles/pp0084a_pdf.pdf
[24] https://www.gsma.com/sas
[25] GSMA, Remote Provisioning Architecture for Embedded UICC, Test Specification, V1, November 2014
[26] http://www.globalcertificationforum.org/certification.html
[27] Formerly the PCS Type Certification Review Board, https://www.ptcrb.com/
[15] https://www.gsma.com/iot/wp-content/uploads/2021/06/IoT-SAFE-Whitepaper-2021.pdf

of cellular network authentication for third-party services. It defines a SIM Applet and their interfaces, and how to use the eSIM as a secure element. This can be useful to store cryptographic materials needed for authentication, identification, and authorization.

The architecture is depicted in Figure 5[28].

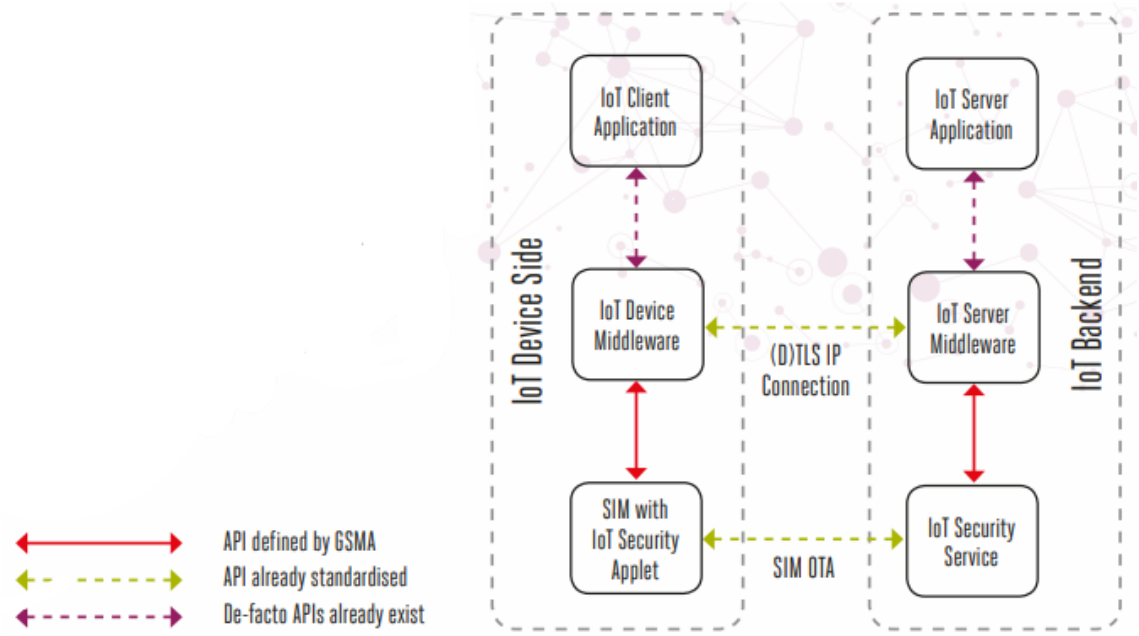

Figure 5 - IoT SAFE Architecture

The components defined by IoT SAFE are the IoT Security Service, the IoT Security Applet, the IoT Server Middleware, and the IoT Device Middleware.

The IoT Security Service module provides both the IoT device and the customer application server with the cryptographic material needed to establish secure channels. The IoT SAFE Security Applet is used to store this cryptographic material. The IoT Server Middleware acts as an interface connecting the IoT Security Server module to the customer application server, and the IoT Device Middleware acts as an interface connecting the IoT SAFE Security Applet to the IoT device.

There are two Free and Open-Source Software IoT device middleware implementations:

- Thales IoT SAFE Middleware library[29]
- Orange IoT SAFE APDU library[30]

And one SSL implementation designed for IoT devices:

- wolfSSL IoT-Safe example[31]

eSIMs (and any other xSIM) are secure elements (SE) and, therefore, can act as the Root of Trust (RoT) in a cryptographic system. A RoT is any element that can be trusted and hold the necessary credentials and keys for the secure lifecycle of the system.

---

[28] https://www.gsma.com/iot/wp-content/uploads/2020/05/IoT-SAFE-Executive-Summary.pdf
[29] https://github.com/ThalesGroup/iot-safe-middleware
[30] https://github.com/Orange-OpenSource/IoT-SAFE-APDU-library
[31] https://github.com/wolfSSL/wolfssl

3.2.2.3 Requirements

Requirement 1.2.1 – IoT eSIM support
ARCADIAN-IoT IoT devices shall support eSIM, which will act as the RoT (store identification credentials and cryptographic material for hardened encryption), act as security enabler and provide cellular connectivity.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
IoT devices
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 1.2.2 – Personal Device eSIM Support
Compliant personal devices shall support eSIM, which will act as the RoT (store identification credentials and cryptographic material for hardened encryption), act as security enabler and provide cellular connectivity.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
Personal devices (smartphones)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 1.2.3 – Receive eSIM profile requests

The eSIM ecosystem shall be able to receive requests for *ARCADIAN-IoT eSIM profiles* from compliant ARCADIAN-IoT devices or services.
Related to Use Case Domain / Category / ID / Name
A1, B1, C1
Requirements Scope (Person/IoT/Apps Services)
IoT devices, personal devices
Requirement preconditions
Req 1.2.1, Req 1.2.2 The device must support eSIM
Requirement postconditions
An ARCADIAN-IoT profile is successfully requested
Requirement Priority
Mandatory

Requirement 1.2.4 – Generate an ARCADIAN-IoT eSIM profile
A novel and specific ARCADIAN-IoT eSIM profile needs to be developed. It will contain identity and authentication elements (related with persons and devices) and cryptographic material for implementing hardened encryption in devices. It will also have methods for securely accessing that RoT information from the device. This profile also needs to be ready to provide connectivity.
Related to Use Case Domain / Category / ID / Name
A1, B1, C1
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Personal devices
Requirement preconditions
Req 1.2.3 An ARCADIAN-IoT profile must be requested
Requirement postconditions
An ARCADIAN-IoT profile is successfully generated
Requirement Priority
Mandatory

Requirement 1.2.5 – Provision profiles to authorized devices
An *ARCADIAN-IoT eSIM profile* shall be provisioned, over-the-air, to authorized devices, when

requested by the device or by an authorized entity.
Related to Use Case Domain / Category / ID / Name
A1, B1, C1
Requirements Scope (Person/IoT/Apps Services)
Apps
Requirement preconditions
Req.1.2.4, Req. 5.2.1 An ARCADIAN-IoT eSIM profile must be successfully generated The device must have authorization to receive the ARCADIAN-IoT eSIM profile
Requirement postconditions
The ARCADIAN-IoT eSIM profile is successfully provisioned, over-the-air, to the authorized device.
Requirement Priority
Mandatory

Requirement 1.2.6 – Update eSIM profile
It shall be possible to securely update an ARCADIAN-IoT eSIM profile over-the-air.
Related to Use Case Domain / Category / ID / Name
A6, A7, B4, C5
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Personal devices
Requirement preconditions
Req. 1.2.5 It must be possible to provision ARCADIAN-IoT eSIM profiles to authorized devices.
Requirement postconditions
The ARCADIAN-IoT eSIM profile is successfully updated over-the-air.
Requirement Priority
Mandatory

Requirement 1.2.7. – Access eSIM profile information
Information in ARCADIAN-IoT eSIM profile needs to be securely accessible from the device where it is hosted.
Related to Use Case Domain / Category / ID / Name

All Domains
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Personal devices
Requirement preconditions
Req 1.2.5 It must be possible to provision ARCADIAN-IoT eSIM profiles to authorized devices.
Requirement postconditions
The device can successfully access ARCADIAN-IoT eSIM profile information.
Requirement Priority
Mandatory

3.2.2.4 Evaluation KPIs

The following KPIs will be used to assess the quality of the component achieved:

1) eSIM acts as an ARCADIAN-IoT RoT.
2) Support identity approaches at hardware level at the eUICC/eSIM.
3) eSIM RoT is an active agent reducing threats impact.

3.2.3 Biometrics

3.2.3.1 Summary

The Biometrics component will be able to identify persons through face recognition for identity management purposes, focusing on drone-based operation scenarios. To do so, it will receive a video feed and will be able to identify faces from an available face database – not necessary that the face image is stored in a centralised database, it could be stored in a user´s SSI wallet and only shared when required.

3.2.3.2 State of the Art

Biometrics have been widely applied to different applications, whilst ARCADIAN-IoT will focus on applying biometrics to drone-based identity management scenarios by exploring AI/ML/data-based approaches in challenging conditions and considering necessary privacy preservation. This drone-based Biometric component will recognise a person (focusing on ARCANDIAN-IoT users such as the drone pilots for authorisation and the user of the Drone Guard Angel use case service) through analysing his/her facial characteristics even in challenging conditions caused by the operation of the drone such as non-frontal face angles, by the natural environments such as low lighting, or partial concealing of a face e.g., by wearing a mask. For instance, the National Institute of Standards and Technology (NIST) of USA has recently tested 100 new facial-recognition algorithms submitted to NIST since mid-March 2020, and the testing results show that the recognition accuracy in many of these existing algorithms has dropped notably with an up to

40% false non-match rate (FNMR) in recognising faces with masks[32]. It is expected that this FNMR would increase significantly due to the distinct operation of drones and the adverse environments as highlighted above.

3.2.3.3 Requirements

Requirement 1.3.1 – Face Database
The algorithm will require the photo of the user to perform his/her face identification against a video feed.
Related to Use Case Domain / Category / ID / Name
Domain A
Requirements Scope (Person/IoT/Apps Services)
Person
Requirement preconditions
Explicit consent of the user to share the photo of his/her face.
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 1.3.2 – Video Feed Reception
The algorithm will require the reception of a video feed coming from the drone in order to allow the biometric algorithm to perform the face identification.
Related to Use Case Domain / Category / ID / Name
Domain A
Requirements Scope (Person/IoT/Apps Services)
IoT / Drone
Requirement preconditions
N/A
Requirement postconditions

[32] NISTIR 8331 DRAFT SUPPLEMENT, "Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms", Mar 2021, available at https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report.pdf.

N/A
Requirement Priority
Mandatory

3.2.3.4 Evaluation KPIs

The following KPIs will be used to assess the quality of the component achieved:

1) Number of frames that can be analysed per second.
2) End-to-End Delay of the whole biometric process.
3) Accuracy achieved in the face identification algorithm (F1-score and similar accuracy metrics).

3.2.4 Authentication

3.2.4.1 Summary

In ARCADIAN-IoT, we aim at extending eSIM ecosystem technologies, keeping at least the same level of security, to provide secure authentication of M2M devices and mobile consumers to relevant IoT third-party services. Furthermore, ARCADIAN-IoT will use multi-factor authentication joining the network credentials with self-sovereign identity mechanisms and novel biometric approaches (described in other sections).

3.2.4.2 State of the Art

This section presents State of the Art that only concerns authentication with network credentials. Other types of authentication are depicted in their own sections.

The concepts of authentication and authorization are usually interconnected. To clarify the differences and their respective roles it is important to offer a clear definition of each concept. Authentication is defined as the verification of the identity of a user, process, or device.[33] Authorization is defined as the right or permission that is granted to a system entity to access a system resource.[34]

OAuth 2.0

OAuth 2.0[35] is an authorization framework that allows users to authenticate towards a remote resource/service. This framework defines four participants: the client, the resource owner, the resource server and the authorization server. The client is the entity that requests access to a protected resource on behalf of the resource owner, and it can only access the protected resource once it has been granted authorization. The resource owner is the entity that can grant permission to the client to access said resource. The resource server is the entity hosting the protected resource, allowing access to the resource when presented with an access token. The authorization server is the entity capable of issuing access tokens after successfully authenticating the resource owner and obtaining permission.

[33] https://csrc.nist.gov/glossary/term/authentication
[34] https://csrc.nist.gov/glossary/term/authorization
[35] https://datatracker.ietf.org/doc/html/rfc6749

OAuth2.0 Protocol Flow

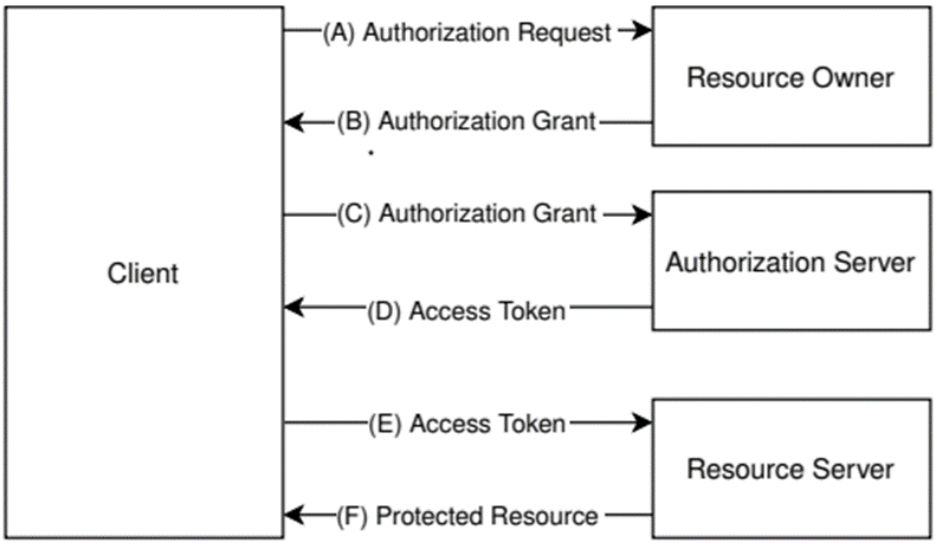

Figure 6 - OAuth Protocol Flow

The interactions between these roles are depicted in Figure 6. **A** marks the start of the interaction between all parties, with a request for authorization to access the protected resource, made by the client to the resource owner. **B** depicts the response to the authorization request, where the resource owner grants the client authorization to access the protected resource. In **C**, the client presents this authorization grant to the authorization server which, after authenticating the client and validating the authorization grant, issues an access token that is sent to the client in **D.** In **E** the client requests the protected resource to the resource server, sending the access token in the request. The resource server validates the access token and responds to the client by allowing access to the protected resource in **F**. An important caveat is that the client works on behalf of the resource owner, meaning that steps **A** and **B** are usually not actual message exchanges between different entities but an end-user, acting as the resource owner, using an application, acting as the client, to access information that he controls on another service/application.

OAuth2.0 Access Token

The access token is the token that proves that the client has the authorization to access the protected resource. This access token has the form of a JSON Web Token (JWT). The access token must be signed or MACed to prove the authenticity or the integrity of the token and it must use the following claims:

1. The JWT contains an “iss” claim, that stands for “issuer” and represents the entity that issued the token.
2. The JWT contains a “sub” claim, that stands for “subject” and represents the entity that is identified by the token.
3. The JWT contains an “aud” claim, that stands for “audience” and represents the authorization server as the intended audience for the token.
4. The JWT contains an “exp” claim, that stands for “expiration time” that limits the time window during which the JWT can be used.

The access token to be considered valid must be a valid JWT and the resource server must be able to validate this token. This validation includes validating the signature and the “aud” claim which must indicate that the token was issued to access the determined protected resource.

Authentication with cellular network credentials

The cellular network is capable of authenticating a SIM card through the use of network credentials. Network credentials are the unique keys/values that allow a SIM card to be authenticated and identified by the cellular network. By leveraging the authentication that the cellular network provides we can authenticate a SIM-equipped device.

Notarizer – Truphone's network credential authentication mechanism

Truphone has a patent pending working solution (patent ID PCT/GB/2021/051093) capable of authenticating IoT devices equipped with a Truphone SIM to a third-party. This authentication mechanism is based on OAuth and leverages the core network capacity to authenticate SIM-Cards.

Protocol Flow

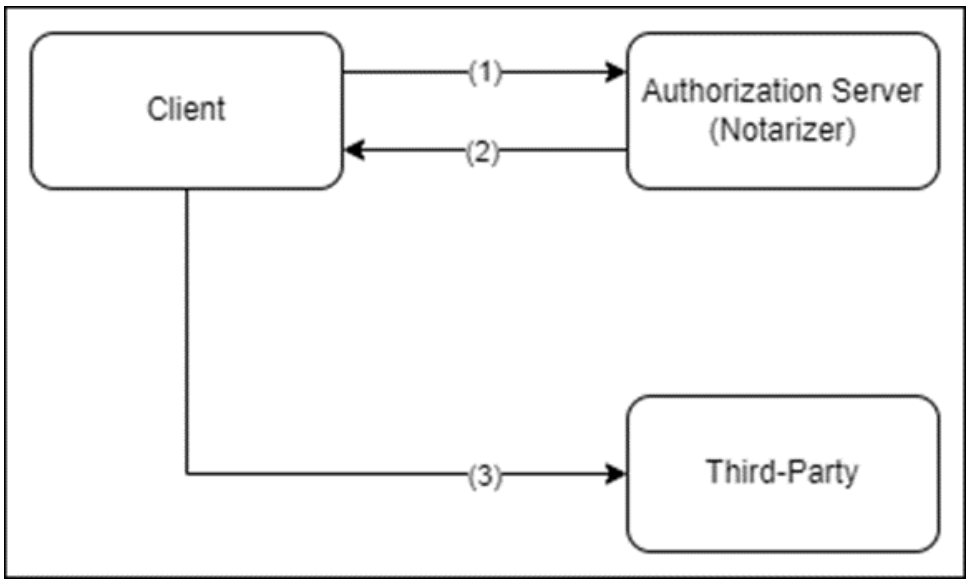

Figure 7 - Notarizer protocol flow

Analyzing the Notarizer protocol flow showcased in Figure 7. In **(1)**, the client asks for a token to the authorization server. In this request, the client will send to the authorization server SIM credentials. Since the authorization server is deployed in Truphone's core network, it has access to the mapping between a certain client's IP address and their SIM credentials, allowing the authorization server to identify the client. In **(2)**, the authorization server responds to this request with the token issued for the client, and finally, in **(3)**, the client uses this token to authenticate itself towards the third-party service.

Custom authenticators

Custom authenticators refer to the process in which a user can directly configure an authentication mechanism when using a Cloud services provider. Instead of using one of the authenticators that the Cloud service provider offers, the user creates its own method of identification, authentication and authorization, and identity and access management will be done using this custom authenticator. Examples of this mechanism exist in Amazon Web Services (AWS) with the

“Custom Authorizer” feature.

A Custom Authenticator trades-off the reliability of a well-known and already implemented authentication system for flexibility. IAM (Identity Access Management) must be performed manually. A Custom authenticator will be necessary in order to create an authentication mechanism that can work with network credentials, SSIs and biometrics.

3.2.4.3 Requirements

Requirement 1.4.1 – Authenticate persons in ARCADIAN-IoT services
Persons should be able to be identified and authenticate in compliant ARCADIAN-IoT services using SSI (DID, VC), network credentials from their personal devices and/or with their biometric characteristics. Some of this information is stored in the personal device RoT and other uses a decentralized approach.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Apps, Services
Requirement preconditions
Req. 1.1.1, Req 1.2.7, Req 1.3.1, Req, 1.3.2 The person must have a Decentralized Identity. The person’s device must be able to access ARCADIAN-IoT eSIM profile information. The person must be able to be identified using biometric characteristics.
Requirement postconditions
The person is successfully authenticated to ARCADIAN-IoT compliant services using either SSI, network credentials or biometric characteristics.
Requirement Priority
Mandatory

Requirement 1.4.2 – Authenticate devices in ARCADIAN-IoT services
Devices (IoT devices and personal devices) should be able to be identified and authenticate in compliant ARCADIAN-IoT services using SSI (DID, VC) and network credentials. Some of this information is stored in the device RoT and other uses a decentralized approach.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Apps, Services
Requirement preconditions

Req. 1.1.1, Req. 1.2.7
Requirement postconditions
The device must have a Decentralized Identity. The device must be able to access ARCADIAN-IoT eSIM profile information.
Requirement Priority
Mandatory

Requirement 1.4.3 – Identify and authenticate apps and services in ARCADIAN-IoT
Compliant apps and services should be able to be identified and authenticate in ARCADIAN-IoT framework with two robust identity mechanisms.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
IoT devices, Apps, Services
Requirement preconditions
N/A
Requirement postconditions
The compliant app or service is successfully identified and authenticated to the ARCADIAN-IoT framework.
Requirement Priority
Mandatory

3.2.4.4 Evaluation KPIs

The following KPIs will be used to assess the quality of the component achieved:

1) Enable, at least 3 multiple simultaneous identification approaches for persons.
2) Support, at least two robust identity mechanisms for devices and apps/services.

3.3 PRIVACY Horizontal Layer (crossing IDENTITY Vertical Layer)

3.3.1 Self-aware data privacy

3.3.1.1 Summary

Within the scope of the Arcadian-IoT project, Martel is developing a component to empower the users to enhance data privacy, in particular by allowing the issuing of privacy policies for data (anonymization, pseudo-anonymization and encryption) leveraging crowdsourcing and historical information.

3.3.1.2 State of the Art

The self-aware data privacy component will leverage different tools to reach its goals: a tool for guaranteeing data privacy (yellow part of the picture below), which can be achieved in several ways according to a recent ENISA (European Union Agency for Cybersecurity) publication,[36] and a recommender tool which will assess data similarity and thus suggest anonymisation policies (blue part in Figure 8).

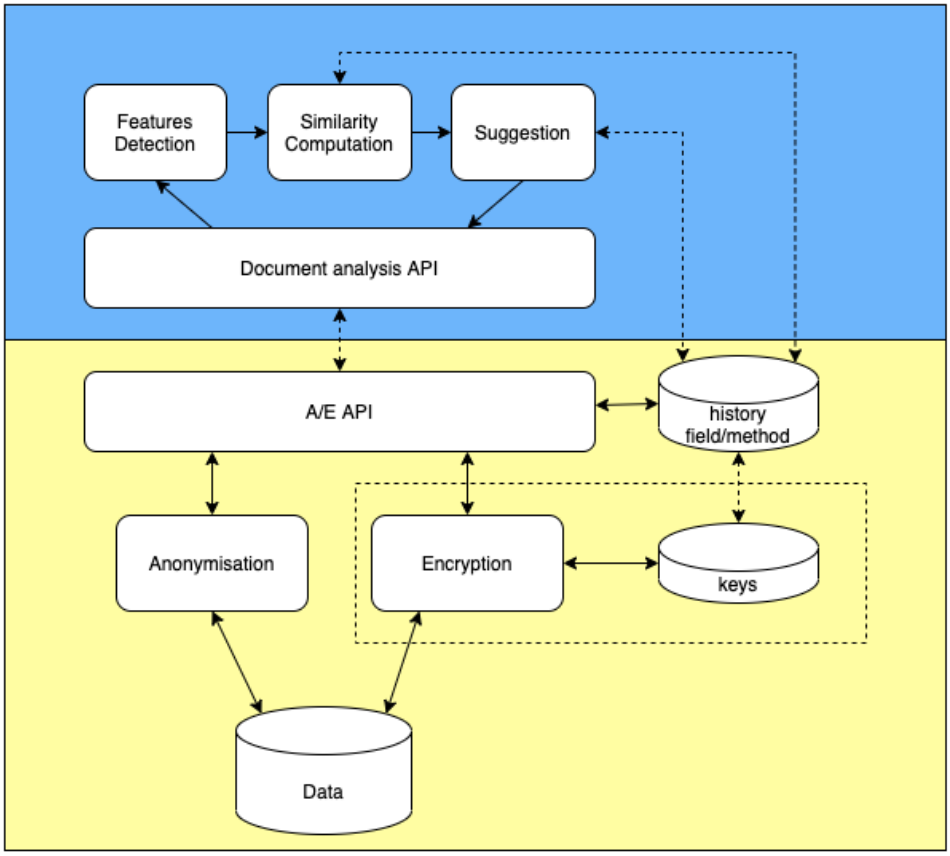

Figure 8 - Self-aware data privacy component draft architecture

A first distinction to make is among “anonymisation”, defined as a process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party and eventually regulated by ISO standard ISO/TS 25237:2017[37] and ”Pseudo-anonymisation”, which is the process by which personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (GDPR, art. 4(5)). Within the framework of ARCADIAN-IoT, both approaches could be applied whereby the most common techniques are based on Random number generator (RNG), Cryptographic hash function, Message authentication code (MAC) and Encryption.

Advanced Encryption libraries like functional- or attribute-based encryption are emerging in the

[36] ENISA, Pseudonymisation techniques and best practices, Recommendations on shaping technology according to data protection and privacy provision, 2019. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport

[37] https://www.iso.org/standard/63553.html

literature to support more dynamic, robust and distributed approaches to data security and these have been studied in the Hardened Encryption component (section 3.5.1). We are therefore defining a combined plan to enable the support and inclusion of Hardened Encryption libraries for the Encryption part of our component (dotted box in the above picture).

When it comes to recommender tools, a set of many different techniques from consolidated Filtering algorithms up to most recent Deep Factorization Machine approaches exist[38] , all involving explicit or implicit feedback (or a combination of the two) and an analysis will be performed within the project to define the best approach to be employed with respect to the data and data format to be treated. When it comes to data and data format, common matching approaches, prerequisite to a successful recommendation, are based on semantic affinity or word distance. At the implementation stage we will test several approaches and select those that will best fit the ARCADIAN-IoT Scenarios and Use Cases.

Data and policies will be represented in de-facto standard for data definition and transport e.g. JSON or XML and this will be harmonized in accordance with the other partners at integration stage.

3.3.1.3 Requirements

Requirement 2.1.1– User defined Policies
An authorized user can access the system and specify for a given data source or data property the security policies that allows to protect the data either when entering into the system or exiting – or both.
Related to Use Case Domain / Category / ID / Name
A1, A3, A4, A5, B2, B3, B6, C1, C2, C3, C4, C5, C6
Requirements Scope (Person/IoT/Apps Services)
App Services
Requirement preconditions
The system should provide access control for users and their role/properties and authorization e.g., OAuth, etc. Policies format (machine readable) should be specified and a validation tool in place. Data source is available.
Requirement postconditions
Polices are successfully stored in the system.
Requirement Priority
Mandatory

Requirement 2.1.2 – Policies Validation

[38] https://d2l.ai/chapter_recommender-systems/index.html

Security policies can be specified in a machine-readable format (e.g., JSON) and validated against a schema interpreter to assess their validity and applicability.
Related to Use Case Domain / Category / ID / Name
A1, A3, A4, A5, B2, B3, B6, C1, C2, C3, C4, C5, C6
Requirements Scope (Person/IoT/Apps Services)
Apps Services
Requirement preconditions
n/a
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 2.1.3 – Data secured
Data sources or data attributes can be secured by a given methodology: anonymization, pseudo-anonymization, encryption and advanced encryption (hardened) based on attribute based encryption.
Related to Use Case Domain / Category / ID / Name
A1, A3, A4, A5, B2, B3, B6, C1, C2, C3, C4, C5, C6
Requirements Scope (Person/IoT/Apps Services)
Apps Services
Requirement preconditions
Data source is available.
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 2.1.4 – Recommender
The system is able to recognise similarity between new data and existing data by key, attributes and/or semantic. This result is eventually displayed to users for facilitating the issuing of security policies.
Related to Use Case Domain / Category / ID / Name

A1, A3, A4, A5, B2, B3, B6, C1, C2, C3, C4, C5, C6
Requirements Scope (Person/IoT/Apps Services)
Apps Services
Requirement preconditions
Data source is available.
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.3.1.4 Evaluation KPIs

The main components will be tested through these KPIs:

1) Performance of the algorithms to secure the data (e.g., speed or robustness).
2) Precision/recall for the recommender algorithms.
3) Usability of the policing issuer (Likert scale).

3.4 SECURITY Horizontal Layer (crossing IDENTITY Vertical Layer)

3.4.1 Flow & behaviour Monitoring

3.4.1.1 Summary

The flow/behaviour monitoring component includes two complementary components: the **network flow monitoring**, operating at the IoT infrastructure side (mapping to Network Intrusion Detection System - NIDS approach), and the **device behaviour monitoring** operating at the device side (mapping to Host Intrusion Detection System HIDS).

The **network flow monitoring** will continuously monitor the infrastructure network for malicious flows in real-time. The component will make use of detection rules in order to perform the detection of malicious threats against the traffic being monitored in the infrastructure. When the threats are detected, new alerts will be generated to inform about that detection. The component will support not only traditional IP networks but also the overlay networks currently being used in cloud infrastructures such as Virtual Extensible LAN (VXLAN), Generic Routing Encapsulation (GRE), Geneva, those currently used in enterprise infrastructures such as VLAN, those currently being used in IoT mobile operator networks such as GTP used in LTE-M and NB-IoT, and those currently being used in non-cellular IoT networks such as LoRa. This component is divided in two different subcomponents. The first one is a state-of-the-art Network Intrusion Detection System (NIDS) such as Snort, Suricata or Bro. And the second one is the Security Flow Monitoring Agent (SFMA) designed as a wrapper to be in charge of providing additional capabilities to the NIDS subcomponent such as the possibility to perform the detection of threats in these new types of networks previous described.

The **behaviour monitoring** sub-component will perform intrusion detection algorithms in lightweight devices, relying on federated AI models performing detection using host data. For such, it will analyze the behavior of devices while respecting user privacy, by taking into account

multiple host data such as device logs, applications' requested permissions, and open sockets/files.

3.4.1.2 State of the Art

Network intrusion detection SoA

Currently, Snort, Suricata and Bro are some of the most advance engines to perform signature-based NIDS. They have been designed to be very effective on traditional IP networks. However, they start showing drawbacks in terms of detection capabilities, support and performance when they are used to perform NIDS in IoT networks, mainly due to their lack of support for the detection of attacks in overlay networks. In this sense, Snort is probably the most advanced one providing elementary support for the overlay networks of VXLAN and GTP. However, none of them provide support for IoT networks and this is where the wrapper created over such NIDS will be used to provide such innovation. These components will allow the detection of Distributed Deny of Service attacks (DDoS).

IoT device intrusion Detection

Previous works demonstrated that an intrusion detection algorithm for IoT applying a deep migration model may lead to shorter response times and higher detection efficiency[39].

Other approaches include a 3-layered IDS system[40], with (1) a layer for classifying the type and profile of every IoT device, (2) a layer for identifying malicious packets on the network and (3) a layer that classifies the type of detected attacks; System evaluation through distinct IoT devices (e.g., cameras, sensor hubs) show good performance, with an F-measure above 90%.

Considering that IoT devices, particularly sensors, have low computational resources, it is crucial for the designed IDS to be lightweight. Authors[41] presented a lightweight hybrid system that combines components running on Android devices, monitoring and gathering data that is transmitted to central servers, where correlation and ML techniques are used to identify malicious behaviour. A similar approach was applied to smart grid context[42], with IDS systems being designed specifically for Advanced Metering Infrastructure (AMI) and Supervisory Control and Data Acquisition (SCADA), and combined with anomaly and signature techniques.

More recently, READ-IoT[43] focuses reliable and integrated event and anomaly detection by relying on a reputation-aware provisioning of detection capabilities, taking into account the vulnerability of the deployment hosts; using an NSL-KDD public dataset and generated date simulating routing attacks, the efficiency of the solution in terms of event detection accuracy and real-time processing was shown.

---

[39] Li, Daming, et al. "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning." *International journal of information management* 49 (2019): 533-545.

[40] Anthi, Eirini et al."A supervised intrusion detection system for smart home IoT devices." *IEEE Int. of Things J.* 2019.

[41] Pedro Borges, et al. "Towards a hybrid intrusion detection system for android-based PPDR terminals." IEEE IM *2017*.

[42] P. I. Radoglou et al., "Securing the Smart Grid: A Comprehensive Compilation of IDPS," IEEE Access, 2020.

[43] A. Yahyaoui, T. Abdellatif, S. Yangui and R. Attia, "READ-IoT: Reliable Event and Anomaly Detection Framework for the Internet of Things," in *IEEE Access*, vol. 9, pp. 24168-24186, 2021, doi: 10.1109/ACCESS.2021.3056149.

3.4.1.3 Requirements

Requirement 3.1.1 – IoT Network Detection
The flow monitoring component will have the capabilities to perform the detection of DDoS attacks in any network segment of the IoT infrastructure, triggering the associated alert.
Related to Use Case Domain / Category / ID / Name
Domain C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
N/A
Requirement postconditions
Attack has been detected
Requirement Priority
Mandatory

Requirement 3.1.2 – User logs access
The behaviour monitoring component must have access to device's user logs in order to detect possible security issues.
Related to Use Case Domain / Category / ID / Name
A, B, C.
Requirements Scope (Person/IoT/Services)
Devices
Requirement preconditions
Device produces operational logs
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 3.1.3 – Device permissions
The behaviour monitoring component must be aware of permissions granted to applications/services accessing the device.

Related to Use Case Domain / Category / ID / Name
A, B, C.
Requirements Scope (Person/IoT/Services)
Devices
Requirement preconditions
Device is able to grant access and/or execution rights to services/apps.
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 3.1.4 – Local model training capabilities
The device should have enough computational resources to support local model training.
Related to Use Case Domain / Category / ID / Name
A, B, C.
Requirements Scope (Person/IoT/Services)
Device
Requirement preconditions
N/A.
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 3.1.5 – Response to anomalies
The behaviour monitoring component should be able to send an alarm, in real time, when anomalous behaviour is detected.
Related to Use Case Domain / Category / ID / Name
A, B, C.
Requirements Scope (Person/IoT/Apps Services)
Device.

Requirement preconditions
Anomalous behaviour must be detected.
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 3.1.6 – Secure communication
The behaviour monitoring component communications should be secured (e.g., using encryption).
Related to Use Case Domain / Category / ID / Name
A, B, C-
Requirements Scope (Person/IoT/Apps Services)
Devices
Requirement preconditions
Encryption mechanisms are available.
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.4.1.4 Evaluation KPIs

The **Flow Monitoring Agent** will be evaluated against the following KPIs:

1) Max number of packets/bytes able to be processed per second without packet losses.
2) Number of network segments suitable to be deployed (Flexibility).
3) Number of IoT technologies/protocols able to be protected (IoT Support).

The **Device Behaviour Monitoring** will be evaluated against the following KPIs:

1) Classification accuracy. The ability of the system accurately to distinguish between intrusions and non-intrusions.
2) Response time of the system when an intrusion occurs.
3) Enable local training in at least 2 different types of devices (e.g., smartphone, IoT GW).

4) Enable Federated AI in at least 2 different types of devices (e.g., smartphone, IoT GW).

3.4.2 Cyber Threat Intelligence

3.4.2.1 Summary

ARCADIAN-IoT will develop a Cyber Threat Intelligence (CTI) platform with a focus on IoT deployments. The CTI component aims at producing, exchanging, and elaborating information about cyber threats and attacks, and their affected entities. CTI systems are strictly necessary in critical infrastructures and they are widely developed nowadays; however, the increase of the number of highly constrained edge devices along with the extended remote connectivity, as resulted in sustainable IoT deployments, determined more stringent requirements of security, privacy, and trust. Although several projects and standardization activities are currently working on new lightweight IoT security protocols, secure connectivity of IoT with cloud backend, distributed trust in IT, etc, CTI systems tailored to IoT deployments are relatively immature technologies. The CTI in the ARCADIAN-IoT framework will support Indicator of Compromise (IoC) generation and sharing by any participating IoT device as well as it will be automatically updated exploiting Opensource intelligence (OSINT) tools such as Shodan, social networks, and dark/deep networks. The CTI will also enable anomaly detection, intrusion detection and prevention, as well as novel and innovative protection mechanisms.

3.4.2.2 State of the Art

The market in Cyber security offers dozens of commercial threat intelligence platforms, such as IBM X-Force Exchange[44], Palo Alto Networks AutoFocus[45], Splunk[46], The Security Fabric[47], etc. However, these solutions integrate external, mostly open, threat information into their proprietary Security protocols and Event Management (SIEM)-like platforms. In addition, they cover a small set of threat intelligence capabilities, and none of them focus on IoT deployments.

Some pilot projects for open-source CTI platforms have been launched recently: e.g., The OpenCTI project[48], Threat Intelligence for Europe, and ECHO's Early Warning System[49]. The OpenCTI project has been developed by the French national cybersecurity agency (ANSSI) and the CERT-EU, and it allows the cyber security actors to structure, store, organize, visualize and share their knowledge about cyber threats. CONCORDIA's Threat Intelligence for Europe and ECHO's Early Warning System have been developing more comprehensive and open platforms to exchange cyber threat warning and incident data. Nonetheless, all these open solutions still focus on traditional deployments with internet hosts.

To the best of our knowledge, there is no CTI platform available in the literature that targets IoT requirements and issues in the fight against cyber threats. For this reason, ARCADIAN-IoT will fill this critical gap and provide a CTI platform that will focus on IoT-specific threat intelligence. The ARCADIAN-IoT CTI component will be developed on MISP and will integrate two parts: (1) an MISP-based CTI platform for IoT (MISP4IoT) and (2) a Privacy-preserved threat information sharing using federated ML (Federated-MISP)

---

[44] https://exchange.xforce.ibmcloud.com/
[45] https://www.paloaltonetworks.com/cortex/autofocus
[46] https://www.splunk.com/
[47] https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric
[48] https://www.opencti.io/
[49] https://echonetwork.eu/echo-early-warning-system-e-ews/

3.4.2.3 Requirements

Requirement 3.2.1 – Threat data collection
The CTI should be able to collect threat data from different sources, local and internal sources (wide variety of different sources)
Related to Use Case Domain / Category / ID / Name
Domain: A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
Threats are detected
Requirement postconditions
Threats data are processed
Requirement Priority
Mandatory

Requirement 3.2.2 – No disclosure of private information
The CTI may need to share information about compromises. Local intelligence in application to not disclose sensitive/private information belonging to users or company.
Related to Use Case Domain / Category / ID / Name
Domain: A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
Sensitive/private information gathered
Requirement postconditions
Threats data are shared with third parties
Requirement Priority
Mandatory

Requirement 3.2.3 – Lightweight Indicators of Compromise
The CTI should support Indicator of Compromise (IoC) generation and sharing by any participating IoT or edge device

Related to Use Case Domain / Category / ID / Name
Domain: A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
IoT or edge device to generate IoC
Requirement postconditions
IoC processing and sharing
Requirement Priority
Mandatory

3.4.2.4 Evaluation KPIs

The CTI will be evaluated against the following KPIs:

1) Number of threat sources supported.
2) Number of IoT technologies/protocols able to share threat data.
3) Number of stakeholders receiving shared data of threats/compromise.

3.5 COMMON Horizontal Layer (crossing IDENTITY Vertical Layer)

3.5.1 Hardened encryption

3.5.1.1 Summary

ARCADIAN-IoT will provide encryption mechanisms to protect data at rest. On one hand, to enable greater flexibility advanced techniques like functional encryption will be used. Functional encryption enables different subjects to decrypt different information from the encrypted files – such flexibility enables easier management of different roles and responsibilities in complex platforms. On the other hand, the security will be hardened by the hardware root of trust approach – the cryptographic keys will be managed by secure elements. Furthermore, the generation and distribution of keys will be synchronized with the decentralized identity paradigm. That is, the identity management and hence the key management will be done in a distributed fashion.

3.5.1.2 State of the Art

Many advanced cryptographic libraries exist and are battle-tested in different environments. However, the libraries are usually not adapted for resource-constrained devices often used in the IoT world. ARCADION-IoT aims to adapt the existing cryptographic algorithms and libraries for the resource-constrained devices. There exist fully-fledged functional encryption libraries like GoFE and CiFEr, but these libraries have not been tested in the IoT context.

To increase the security and the trustworthiness, secure elements enabling hardware-based root of trust are being introduced to many modern devices. To the best of our knowledge no connection between secure root-of-trust elements and modern cryptographic approaches, like functional

encryption, have been established yet.

Furthermore, standard approaches for key management depend on a central authority (server) delegating all the rights. Since such an approach can be highly problematic in case of a failure or security breach, decentralized identity management using blockchains is gaining popularity. Merging the distributed approach with modern cryptographic tools and hardware-based protocols is a challenge to be addressed.

Requirement 4.1.1 – Encryption mechanism
If a device or server needs to secure the data it produces, an efficient and lightweight mechanism must be available to encrypt the data. If necessary, the data can be encrypted with specified privacy policy, defining the rights to access the data. If possible, the encryption mechanism should use only keys secured in a secure element, enabling hardware-based root-of-trust.
Related to Use Case Domain / Category / ID / Name
A3, A4, A5, A6, A7, B2, B3, B4, B7, B8, C3, C4
Requirements Scope (Person/IoT/Apps Services)
Person/IoT/Apps Services
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 4.1.2 – Secure key-generation
A secure and a privacy aware mechanism for generating cryptographic keys and hence delegating access to the data needs to be implemented. The key managing protocol needs to be scalable to support many IoT devices securing their data with minimal interaction with the key provider. If possible, keys should be distributed using a secure network to the secure element of a device. The key delegation should be synchronized with the decentralized identity of the entities.
Related to Use Case Domain / Category / ID / Name
A1, A2, A6, A7, B1, B6, C1, C11, C12
Requirements Scope (Person/IoT/Apps Services)
Person/IoT/Apps Services

Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.5.1.3 Evaluation KPIs

The requirements will be evaluated with the following KPIs:

1) The devices and servers will be able to connect to the Arcadian-IoT platform and obtain all the cryptographic keys needed.
2) Devices will be able to efficiently encrypt their data for storage or recovery with clear policy who can access the data.
3) Only specified users of Arcadian-IoT platform will be able to access the data for analysis or recovery.
4) Keys will be managed in a secure way using hardware-based root-of-trust if possible.

3.6 TRUST Vertical Layer

3.6.1 Verifiable Credentials

3.6.1.1 Summary

ARCADIAN-IoT will provide an identity management solution that is built on W3C Verifiable Credentials specification[50] that is a core standard that is helping to facilitate the Self-Sovereign Identity (SSI) approach in decentralising identity management. The solution enables trusted registration of users through the issuing of identity claims as Verifiable Credentials to their respective secure crypto based digital identity wallets without depending on centralised Identity Providers with its inherent privacy risks. In turn, these credentials can be later presented by the user to services and apps which require to authenticate the user in a trusted crypto based manner that only the holder of these credentials can do (based on the fact they were issued to the wallets Decentralised Digital Identity based in the DLT, as described in section 3.1.1).

The SSI identity management solution will provide the core building blocks for issuing, presenting and verifying credentials as per the W3C model shown below.

[50] W3C, Verifiable Credentials Data Model 1.0, Website, https://www.w3.org/TR/vc-data-model/, retrieved 13 Oct 2021

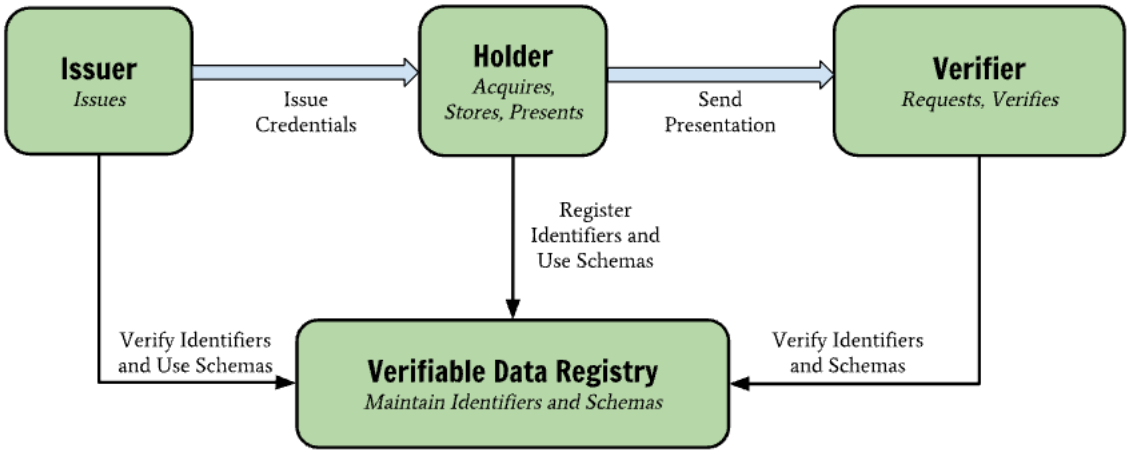

Figure 9 - W3C model

3.6.1.2 State of the Art

The Self-Sovereign Identity landscape in recent years has been dominated by a few innovative companies such as uPort, Jolocom, Evernym etc. all with their own specific proprietary implementations and technology. Therefore, the solutions available today suffer very much from competing protocols and immature standards to create SSI islands. However, the landscape of large and small organisations and governments pushing SSI has grown and much needed standards are maturing. Most relevant to Europe, is EBSI that has a primary objective to create and define standards for a European SSI Framework (ESSIF) to promote decentralised identities and interoperability among vendors and their digital wallet solutions, while aligning with eIDAS and the GDPR so to ensure that ESSIF benefits from existing legal frameworks[51]. Indeed, Europe is currently proposing a new regulatory framework to enable citizens to be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone.

To get a comprehensive view of the current SOTA the reader is encouraged to read this recent survey of SSI ecosystems[52]. In this survey you will see mentioned the Hyperledger Consortium which is an umbrella project managed by the Linux Foundation and is an open-source community focused on the development of a suite of stable frameworks, tools and libraries for enterprise-grade blockchain deployments.

The SSI solution to be implemented in ARCADIAN-IoT will be based on Hyperledger Aries which provides a shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. It can use blockchain to provide a trust anchor for peer-to-peer decentralised identity interactions and at the same time is blockchain agnostic.

The Decentralized Identity Foundation (DIF) promotes interoperability in the SSI domain and as such provides guidance to working groups producing standards, specifications, reference implementations and demonstrations hosted by community organizations including but not limited to IETF, W3C, W3C CCG, Hyperledger, Trust over IP. Hyperledger Aries is very active in DIF to

51 EC, *Commission proposes a trusted and secure Digital Identity for all Europeans*, Website, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663, retrieved 13 Oct 2021
52 Soltani, Reza, (2021), *A Survey of Self-Sovereign Identity Ecosystem*, https://www.hindawi.com/journals/scn/2021/8873429/, retrieved 13 Oct 2021

promote interoperability, for example a protocol enabling SSI agents to talk to each other called DIDComm was born in the Aries project, and its latest version was the outcome of a working group collaboration at DIF

3.6.1.3 Requirements

Requirement 5.1.1 – Verifiable Credential management
To provide Verifiable Credential based identity management to enable secure and authenticated identity and other claims needed by the services and apps in the IoT ecosystems
Related to Use Case Domain / Category / ID / Name
A1, A2, A7 *B5* *C1, C2, C4, C5, C7*
Requirements Scope (Person/IoT/Apps Services)
Person /Personal devices
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.6.1.4 Evaluation KPIs

1) Number of issued VCs.
2) Number of presented VCs received.
3) Number of VCs verified successfully.
4) Number of VCs failed verification.
5) Number of VCs revoked.
6) Number of VCs suspended.
7) Number of VCs re-activated.

3.6.2 Authorization

3.6.2.1 Summary

In ARCADIAN-IoT, we will leverage network-based policy enforcement tools, to enable and enforce novel processes of dynamic authorization throughout ARCADIAN-IoT ecosystems. Authorization is expected to be enforced according to the entities' trustfulness (e.g., reputation), automatically reacting to incident events or proactively acting in the presence of threats by blocking accesses from/to the network (e.g., blocking unauthorized accesses to sensitive data or

unauthorized control of devices or services behaviour).

3.6.2.2 State of the Art

State of the art authorization components are composed of three parts: (1) Identity and Access Management (IAM) with the aim to devise an information system and the dynamic processes that define the roles and permissions in the ecosystem, specifying *who/what* (person/object) is authorized to perform *which action* in *where*. (2) Authentication where the roles and permissions are matched with the authentication mechanisms. (3) Adds dynamic and automatized processes to the authorization, by adding the entities reputation, as well as healing and federated AI models' results, which may lead to authorization changes. The result is a component that manages dynamically the authorization information, orchestrating other components to define the operations an entity can perform in a specific system or with a specific device, in a given moment.

In today's network architectures, authorization, policy, and billing are already a focus point. 3GPP's Policy and Charging Control (PCC) architecture[53] provides access, resource, and quality of service (QoS) control[54] to mobile networks. Two components of this architecture are the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF).

PCRF acts as the policy manager of the network, the central point of decision that provides policy control and flow-based charging control decisions. The PCEF usually lives in the serving gateway, can offer packet inspection capabilities, and enforces the rules provided by the PCRF. Besides these two components, an Application Function (AF) interacts with other applications and services that require a dynamic PCC[55].

3GPP's PCC architecture describes an AF as "an element offering applications that require dynamic policy and/or charging control over the IP CAN (IP Connectivity Access Network) user plane behaviour." The Application Function extracts session information and media-related information from the application signalling and provides application session-related information to the PCRF using the Rx protocol[55] [56]. This information is the part of the inputs used by the PCRF for the Policy and Charging Control Decisions and the rules engine can be triggered by one of these messages[56].

[53]https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810
[54]https://www.netmanias.com/en/post/techdocs/10997/lte-pcrf/policy-and-charging-rules-function-pcrf-in-lte-epc-core-network-technology
[55]https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/3gpp-policy-charging-control-provisioning-accounting.html
[56]https://www.netmanias.com/en/post/techdocs/10997/lte-pcrf/policy-and-charging-rules-function-pcrf-in-lte-epc-core-network-technology

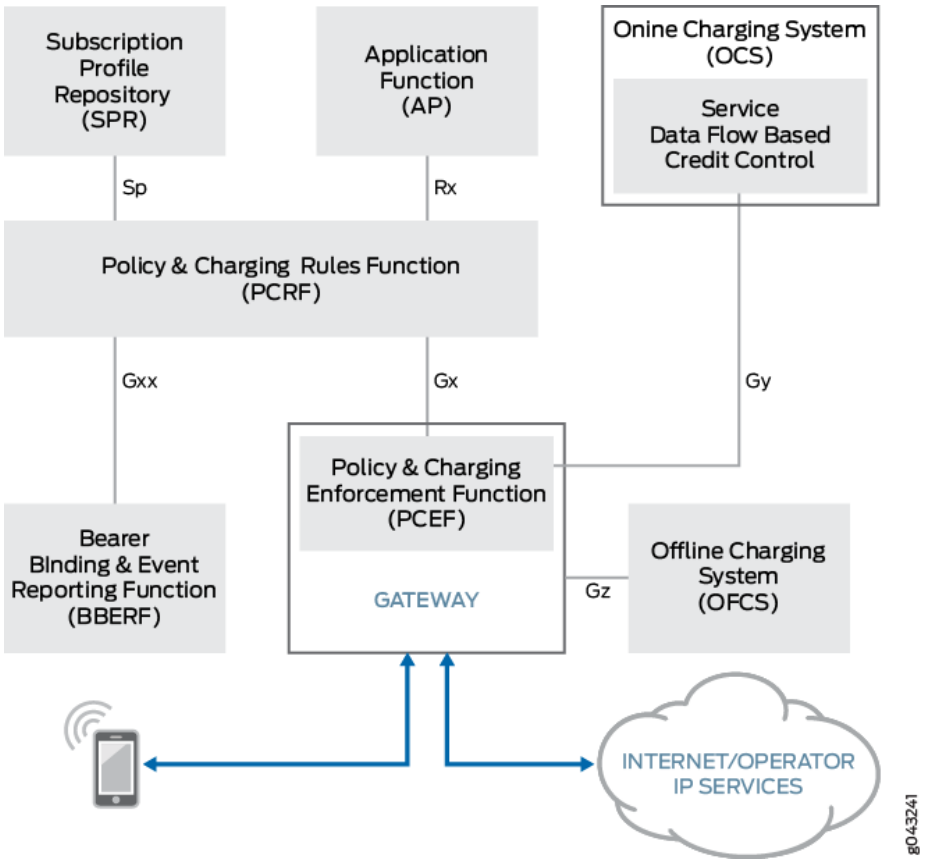

Figure 10 - 3GPP PCC Architecture Overview[55]

Although the Rx interface is DIAMETER-based, efforts have been made by the 3GPP to provide a RESTful approach, with XML as the content body format, to these functions. In this case, a Protocol Converter (PC) acts as the middleman between the AF and the RX-speaking PCRF[57].

It is worth noting that there are two types of PCC rules, predefined and dynamic. The former is already set up in the PCEF and can only be activated or deactivated by the PCRF, while the latter can be provisioned by the PCRF via Gx interface to the PCEF[58] and can be activated, modified, and deactivated in runtime.

In the context of ARCADIAN-IoT, PCRF/PCEF solutions can be leveraged to efficient and dynamically route and prioritize network traffic[54] as a mean of providing authorization inside the network.

PCRF/PCEF uses policy-based authorization, however, as seen in[59], it is possible to build a mixed authorization system that mix static policy-based authorization with dynamic reputation-based authorization. This system combines the advantages of both systems to create a flexible authorization framework.

Static policy-based authorization schemes can take three forms: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Capability-Based Access Control (CapBAC).

In RBAC every user has at least one role and resources can only be accessed by users of a

[57]https://www.3gpp.org/more/1629-rx_interface
[58]https://www.netmanias.com/en/?m=view&id=techdocs&no=11863
[59]http://rewerse.net/publications/download/REWERSE-RP-2005-116.pdf

determined role. ABAC defines an authorization model in which users have multiple attributes that will then be used to check if the user has access to a determined resource. CapBAC states that for users to access a determined resource they need to present a capability that shows that they can access it; this capability is traditionally a key or a token.

3.6.2.3 Requirements

Requirement 5.2.1 – Dynamic network-based authorization enforcement
A network-based enforcement tool (placed in the core network) will control devices, persons, and services access (I/O) to Internet resources based on those entities' reputation/trustfulness, ensuring, for example, that compromised devices just access (or are accessed by) recovery services.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
Person/IoT/Apps/Services
Requirement preconditions
Req 1.4.1, Req 1.4.2, Req. 1.4.3, Req 5.3.3 A person must be authenticated by the ARCADIAN-IoT framework. A device must be authenticated by the ARCADIAN-IoT framework. An app/service must be authenticated by the ARCADIAN-IoT framework. An entity reputation must be stored by a trustable mechanism.
Requirement postconditions
Network-based dynamic authorization is enforced to persons, devices and apps/services.
Requirement Priority
Mandatory

Requirement 5.2.2 – Dynamic RoT/eSIM authorization enforcement
ARCADIAN-IoT eSIM profile shall have methods for enforcing security authorization60.
Related to Use Case Domain / Category / ID / Name
All domains
Requirements Scope (Person/IoT/Apps Services)
IoT
Requirement preconditions

60 Details removed for allowing potential IPR protection

Req 1.2.6, Req 5.2.1 It must be possible to update ARCADIAN-IoT eSIM profiles over-the-air.
Requirement postconditions
The updated ARCADIAN-IoT eSIM profile is able to enforce authorization 61.
Requirement Priority
Mandatory

3.6.2.4 Evaluation KPIs

The following KPI will be used to assess the quality of the component achieved:

1) Authorization component is able to enforce ARCADIAN-IoT trust models for devices, services and persons.

3.6.3 Reputation Systems

3.6.3.1 Summary

The reputation system component provides a trust model for entities (e.g., objects, persons and applications/services). It will model reputation considering the trust properties of the ARCADIAN-IoT trust plane, which will rely on the interactions between intra- and inter-entities, either of the same type (object-object), or different types (person-object).

The established trust model will be based on the behaviour of devices (assessed by the attestation, behaviour monitoring and federated cybersecurity models), the interactions between entities (e.g., how a person interacts with a device), the mobility of nodes/objects and considering the resources of IoT devices. In ARCADIAN-IoT, the focus will mainly be on two features:

- To enable decentralized trust/reputation models (Distributed Trust and Reputation Management System) based on blockchain for exploiting its tamper-proof data capabilities;
- To mitigate the drawbacks regarding lookup time and storage footprint in blockchains (e.g., exploring BigChainDB, multi-level reputation scoring systems based on rewards / kudos).

3.6.3.2 State of the Art

Online reputation systems have evolved to rating systems, where users rate each other based on behaviour[62], but have known exploitability flaws[63]. Reputation systems are typically based on ratings provided by persons; however, more recently, reputation systems have made their way to

61 Details removed for allowing potential IPR protection

[62] Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. Reputation systems. *Communications of the ACM*, 2000.

[63] Dini, Federico, and Giancarlo Spagnolo. "Buying reputation on eBay: Do recent changes help?" *International Journal of Electronic Business* 7.6 (2009): 581-598.

P2P networks[64,65] and ad-hoc networks[66,67]. In the context of IoT systems, nodes and machines are autonomous and distributed, and consequently exposed to attacks (e.g., physical tampering, DoS), thus requiring mechanisms to hold and assess trust in M2M communications[68].

Reputation systems represent one important mean for identifying compromised or malicious devices, as these can propagate unwanted content to others (e.g., malware), or even steal sensitive and private information[69,70]. Reputation models to identify malicious devices have been proposed[71], where each device computes trustworthiness information based on direct experience with others, and the reputation information is shared across the network via hash tables. Other works proposed models intended at protecting privacy and feedback scores of devices while calculating trust and reputation[72]. One of the models is based on the Public Key Cryptography and uses an additive homomorphic scheme for scores' integrity protection – more computationally efficient -, while the second model relies on the additive paillier-cryptosystem providing better security.

Other previous works include a trust and reputation model that employs distributed probabilistic neural networks to identify trustworthy and malicious devices[73]. Their model predicts scores for new devices based on their characteristics, in an attempt to overcome the cold start problem, and evolves using ML techniques. Computation is distributed, handled by the devices, and can be adapted to devices of various capabilities and types. Recent surveys[74], point out that centralized architectures for reputation systems do not accommodate the dynamics of IoT systems and present a single point of failure. Additionally, the distributed architectures for reputation can have different approaches (e.g., fog, cloud), but need to consider trust models that are efficient, scalable and which support the mobility of nodes.

Different reputation models exist and can consider the context on which reputation information is devised, or considering the relations between different parties[75], as depicted in Figure 11.

---

[64] Wang, Yao, and Julita Vassileva. "Trust and reputation model in peer-to-peer networks." *IEEE P2P2003*.
[65] Xiong, Li, and Ling Liu. "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities." *IEEE transactions on Knowledge and Data Engineering* 16.7 (2004): 843-857.
[66] Mejia, Marcela, et al. "A review of trust modeling in ad hoc networks." *Internet Research* (2009).
[67] Azer, Marianne A., et al. "A survey on trust and reputation schemes in ad hoc networks." *Third International Conference on Availability, Reliability and Security*. IEEE, 2008.
[68] Cha, Inhyok, et al. "Trust in M2M communication." *IEEE Vehicular Technology Magazine* 4.3 (2009): 69-75.
[69] Sivaraman, Vijay, et al. "Smart-phones attacking smart-homes." *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 2016.
[70] Yu, Tianlong, et al. "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things." *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. 2015.
[71] Nitti, Michele, Roberto Girau, and Luigi Atzori. "Trustworthiness management in the social internet of things." *IEEE Transactions on knowledge and data engineering* 26.5 (2013): 1253-1266.
[72] Yan, Zheng, et al. "Two schemes of privacy-preserving trust evaluation." *FGCS,* 2016, 175-189.
[73] Asiri, Sarah, and Ali Miri. "An IoT trust and reputation model based on recommender systems." *2016, IEEE PST*.
[74] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," IEEE Access, vol. 8, pp. 60117–60125, 2020.
[75] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *J. Parallel Distrib. Comput.*, vol. 75, pp. 184–197, 2015.

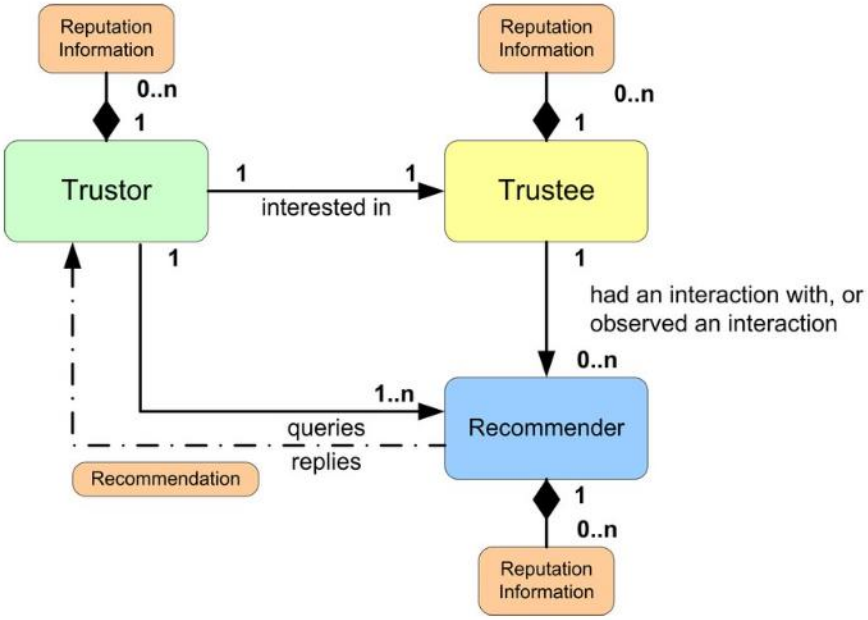

Figure 11 - Reference model for reputation systems

The entities in the reference model of reputation systems are aligned with the architecture for attestation (see subsection 3.6.4), with trustor, trustee and the recommender. The trustor is an entity that decides to trust the trustee entity. For such trust decision, the trustor relies on the reputation of the trustee. The information of reputation can be based on previous interactions, and if no previous interaction, or no reputation information exists, then the trustor queries the recommenders.

The recommenders can build trust by considering:

1. Previous interactions;
2. Observing the interactions between parties;
3. Collecting information from other sources (considered trustful).

The reputation score, which establishes the reputation information in an objective fashion, can be used by trustors. The reputation score can be computed with aggregation mechanisms[76], that compute the score based on weighted sum, inference approaches, regression analysis and flow models. In the weighted sum approach, the ratings are summed according to a weight. This approach is followed by eBay. The inference approach employs techniques like fuzzy logic, Bayesian inference and belief theory. Within the fuzzy logic the reasoning is approximate rather exact, assuming uncertainty. The Bayesian inference employs probabilistic values which are determined considering the observations that occurred and possible future interactions. The Belief theory provides means for objective metrics to represent subjective beliefs. The Regression analysis employs statistics to measure/estimate the relations between trust and entities. The flow models aggregate reputation based on the overall network opinion. For instance the Google PageRank algorithm follows this approach, as it increases the rank of a page considering the flows (in other web pages) pointing to a web page. The links in the web page being ranked that point to other pages lead to a decrease in the reputation score.

[76] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. Khan, and M. K. Khan, “Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges,” *J. Netw. Comput. Appl.*, vol. 145, no. September 2018, 2019.

3.6.3.3 Requirements

The requirements of the Reputation System are summarized in the following subsections

Requirement 5.3.1 – Information of Entities identification
The reputation system needs to be aware of the entities enrolled or interaction with the Arcadian-IoT platform. Such entities include persons, as an example the clients of the DGA in domain A, the medical IoT devices in domain C, or the middleware services in domain B. This requirement leads to the need of identifying entities in the ARCADIAN-IoT platform.
Related to Use Case Domain / Category / ID / Name
Domains A, B and C
Requirements Scope (Person/IoT/Apps Services)
Persons, IoT devices, Applications/Services
Requirement preconditions
Entities are registered in the ARCADIAN-IoT platform or in the services supported by the ARCADIAN-IoT platform.
Requirement postconditions
The reputation system has access to the IDs that are used to identify the diverse entities. For instance, if the object is identified by the eSIM IMEI, then the reputation system should be aware of the value of this IMEI's identifier value.
Requirement Priority
Mandatory

Requirement 5.3.2 – Information of Entities interactions
The reputation system needs to be aware of the interactions between entities enrolled or interaction with the ARCADIAN-IoT platform. Such interactions can be intra- or inter- entities and can be exemplified as successful logins (person-service), or performing user recognizing through image analysis (device-user). In practical terms such requirement leads to the need of having a message bus to sharing data with reputation systems.
Related to Use Case Domain / Category / ID / Name
Domains A, B and C
Requirements Scope (Person/IoT/Apps Services)
Persons, IoT devices, Applications/Services
Requirement preconditions
Entities are registered in the ARCADIAN-IoT platform or in the services supported by ARCADIAN-IoT platform.
Requirement postconditions
N/A

Requirement Priority
Mandatory

Requirement 5.3.3 – Trustable storage mechanisms for reputation
The reputation system requires trustable mechanisms to store the reputation of entities. The storage mechanisms should be distributed to avoid single point of failures.
Related to Use Case Domain / Category / ID / Name
Domains A, B and C
Requirements Scope (Person/IoT/Apps Services)
Persons, IoT devices, Applications/Services
Requirement preconditions
A trustable storage mechanism is in place and provides APIs to enable storage of reputation information.
Requirement postconditions
N/A
Requirement Priority
Optional (assuming the reputation system stores information in a centralized fashion).

Requirement 5.3.4 – Service registration in the reputation systems
Services needing reputation information should register, that is express their intent to receive reputation information. Such registration should also include information on how the reputation information should be provided for the different entities. As an example, the client aiming to use the DGA service needs to know if the service is trustworthy (reputation is considered as trust or distrust) or is considered in a rating scale (i.e., 1 to 5, where 5 means the maximum reputation value).
Related to Use Case Domain / Category / ID / Name
Domains A, B and C
Requirements Scope (Person/IoT/Apps Services)
Persons, IoT devices, Applications/Services
Requirement preconditions
N/A
Requirement postconditions
Upon their registration in the reputation system, the reputation system must determine
Requirement Priority

Optional (assuming the reputation system will only provide an absolute value for reputation).

3.6.3.4 Evaluation KPIs

The reputation system can be evaluated through the following KPIs:

1) Number of messages analysed per second to determine reputation values, unit: messages per (s).
2) Time required to determine reputation, unit: (s).
3) Number persons, objects, services supported by the reputation system, unit: n.º of entities.
4) Computational resources consumed to determine reputation, unit: %of CPU, % of Memory, % of storage, bytes of Input/output.

3.6.4 Attestation

3.6.4.1 Summary

Attestation mechanisms rely on schemes that provide evidence on the integrity of the components and the trustworthiness of services through distributed and scalable approaches. ARCADIAN-IoT provides attestation through challenge-response protocols[77] that consider secure and distributed approaches. ARCADIAN-IoT further enhances attestation mechanisms by considering recent developments towards the support of multiple verifiers in the attestation procedures and the latest recommendations on remote attestation procedures. The proposed mechanisms minimize the attestation's impact on devices and provide functional attestation solutions.

3.6.4.2 State of the Art

ARCADIAN-IoT supports remote and functional attestation mechanisms, following the attestation architecture specified by the IETF Remote Attestation procedures (RATS) working group[78]. This enables technology independence and provides the ability to leverage Root of Trust (RoT) concepts such as Trusted Platform Module (TPM)[79] (in the eSIM secure elements and crypto chipsets). TPMs are often used to store keys and identification information securely. For instance, Samsung Knox is a kind of RoT mechanism used for mutual attestation in home environments. It is aligned with Trusted Execution Environments (TEE) and assures that attestations procedures have not been modified[80]. However, this approach is limited to Samsung devices[81,82]. As such, ARCADIAN-IoT attestation mechanisms should also consider a broader range of devices and not

[77] Steiner, R. V., & Lupu, E. (2016). Attestation in wireless sensor networks: A survey. ACM Computing Surveys (CSUR), 49(3), 1-31.
[78] IETF RATS, available at: https://datatracker.ietf.org/wg/rats/about/
[79] Trusted Computing Group, Trusted Platform Module (TPM) Summary, available online: https://trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
[80] J. Ahn, I.-G. Lee, and M. Kim, "Design and Implementation of Hardware-Based Remote Attestation for a Secure Internet of Things," Wirel. Pers. Commun., no. 0123456789, Apr. 2020.
[81] E. Dushku et al., "SARA: Secure Asynchronous Remote Attestation for IoT Systems" IEEE Tr. Inf. For. Secur., 2020.
[82] M. Ammar, M. Washha, and B. Crispo, "WISE: Lightweight Intelligent Swarm Attestation Scheme for IoT (The Verifier's Perspective)," Int. Conf. Wirel. Mob. Comput. Netw. Commun., vol. 2018-Octob, 2018.

limited to a specific Operating System, such as the Google SafetyNet Attestation API[83]. In addition, the employment of such APIs also needs to be performed with Trusted servers, to avoid misusing the potential features of such APIs.

The attestation component considers the heterogeneity regarding devices' capabilities, and efficient remote integrity verification and challenge-response mechanisms are enabled by design. The evidence provided by such mechanisms - regarding the proof of devices' properties (e.g., operational state, identity) - rely on cryptographic routines of the hardened encryption component, present in the Common layer, and described in Section 3.5.1, to secure its transmission to the verifier nodes and to sign the evidence, protecting it against modifications.

Remote attestation mechanisms are employed in IoT systems due to the limited capabilities of IoT devices. These mechanisms assess the consistency of IoT devices, applications and services, employing challenge-response approaches issued by a verifier node towards many devices. Other mechanisms implement a hybrid approach using hardware and software resources. Attestation is based on secure hardware like TPM or secure elements[84], with the drawback of not being suited to low-resource devices[85].

The software-based approaches commonly fail to address identity authenticity, focusing instead on SW integrity. Additionally, attestation mechanisms lack support for device mobility and are prone to attacks, especially those targeted to the verifier nodes[86]. On the other hand, the attestation mechanisms must also consider scenarios with intermittent connectivity, where lightweight message aggregation mechanisms are required to convey evidence[87].

ARCADIAN-IoT will consider flexible, efficient, and scalable solutions for the remote integrity verification and challenging mechanisms, for instance, relying on secure publish/subscribe models[88] to convey evidence for integration in the reputation system towards assessment of trust, as documented in Section 3.6.3, for the reputation systems' component.

3.6.4.3 Requirements

Requirement 5.4.1 – Attestation pre-installation
In order to enable Remote Attestation procedures, the (IoT) device must have or enable Attestation component pre-installation.
Related to Use Case Domain / Category / ID / Name
A, C

[83] M. Ibrahim and A. Bianchi, "SafetyNOT : On the usage of the SafetyNet Attestation API in Android," pp. 150–162, 2021.

[84] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G Security in 3GPP," pp. 181–186, 2017.
[85] W.Feng et al."AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS" 2018.
[86] Cristina Alcaraz, "Security and Privacy Trends in the Industrial Internet of Things", Springer ASTSA, 2019.
[87] M. M. Rabbani, "Remote Attestation for Secure Internet of Things Acknowledgments," 2019.
[88] M. Conti, M. Hassan, … M. R.-P. of the, and undefined 2019, "RICe: Remote Attestation of Internet of Mobile Things in Information Centric Networking," *Researchgate.Net*, no. February 2020, 2019.

Requirements Scope (Person/IoT/Apps Services)
Device (Attester) Service (Relying party, Verifier)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 5.4.2 – Serialization
A common serialization format should be used for both Evidence and Attestation Result, in order to minimize code footprint and attack surface area.
Related to Use Case Domain / Category / ID / Name
A, C.
Requirements Scope (Person/IoT/Apps Services)
IoT Device / Smartphone / Drone
Requirement preconditions
Both an Attester, a Verifier and a Relying Party must be involved.
Requirement postconditions
N/A
Requirement Priority
Optional

Requirement 5.4.3 – Watchdog timer
A watchdog timer should be implemented in a protected environment such as TPM to receive regular and up to date Attestation Results.
Related to Use Case Domain / Category / ID / Name
A, C.
Requirements Scope (Person/IoT/Apps Services)
IoT Device / Smartphone / Drone
Requirement preconditions

Availability of TPM in the device.
Requirement postconditions
When watchdog timer reaches zero, a platform-reset is triggered.
Requirement Priority
Optional

Requirement 5.4.4 – Protocol data integrity
The integrity of Evidence and Attestation Results should be protected (i.e., either via signing or a secure channel)
Related to Use Case Domain / Category / ID / Name
A, C.
Requirements Scope (Person/IoT/Apps Services)
IoT Device / Smartphone / Drone
Requirement preconditions
Mechanisms for integrity protection should be available
Requirement postconditions
N/A
Requirement Priority
Optional

Requirement 5.4.5 – Attestation procedure confidentiality
Confidentially of Evidence and Attestation Results should be protected via encryption.
Related to Use Case Domain / Category / ID / Name
A, C.
Requirements Scope (Person/IoT/Apps Services)
IoT Device / Smartphone / Drone
Requirement preconditions
Encryption mechanisms should be available
Requirement postconditions
N/A
Requirement Priority

Optional

3.6.4.4 Evaluation KPIs

1) Remote attestation (i.e., Attester component) supporting at least one of ARCADIAN-IoT TPMs.
2) Remote attestation (i.e., Attester component) supporting at least 2 types of ARCADIAN-IoT devices / platforms.

3.7 PRIVACY Horizontal Layer (crossing TRUST Vertical Layer)

3.7.1 Federated AI

3.7.1.1 Summary

ARCADIAN-IoT will develop a federated Artificial Intelligence (AI) module to enable privacy preservation in IoT deployment when sensitive information needs to be aggregated and analyzed by third parties while kept private. Federated AI is a new technique in the machine learning domain which allows to train a distributed model over multiple devices such that the input data is locally processed and not shared among the parties. In centralized federated AI, a central server coordinates the stages of the training process and aggregates local models to a global model at regular intervals. Federated AI is well suited for building common models from IoT data while preserving the privacy of local data sets. However, the solutions currently available require balanced data, independently and identically distributed over the clients. This is not the case in IoT deployments; in fact, IoT usually offers a wide range of diversity of data produced/collected by each end device, in terms of data granularity, data volume, data quality, data acquisition rate, etc. This leads to degraded performance of the federated AI models. For this reason, the federated AI component in the ARCADIAN-IoT framework will include data balancing techniques in the federated setting. In addition, novel model aggregation schemes will be investigated taking data imbalance into account.

3.7.1.2 State of the Art

Federated AI models are currently being adopted in several domains with high restrictions for privacy preservation, e.g., smart manufacturing, healthcare, etc.[89]. Classical federated AI approaches obtain high performance when trained on data with homogeneous statistical distributions. However, the statistical conditions required on the input data to federated models contrast with the statistics observed in data from real IoT deployments; in fact, IoT networks usually consist of multiple device types and environments which introduce a significant bias and variance in the estimate of the full gradient[90]. To overcome this challenge, several data balancing schemes have been suggested. We identified two main strategies for data balancing: (i) data

[89] https://musketeer.eu/project/
[90] Battou, Léon “Large-scale machine learning with stochastic gradient descent”, Proceedings of COMP-STAT’2010.

augmentation[91] and (ii) small subset sharing[92]. In data augmentation, new samples are generated with statistical models for the data from the less numerous classes in order to restore balance; unfortunately, these solutions are not general enough to be deployed in IoT contexts. On the other side, solutions based on small subset sharing determine some privacy violation.

Another critical aspect in this domain is the cost related to the communications between the parties involved in the federated process. Traditional federated AI approaches determine the transmission of significant amount of data between the clients and the server[93] which also involves high computational cost for encryption methods; however, strict constraints on bandwidth and power resources in IoT deployments encouraged for investigation of new lightweight federated solution with low computational and communication cost.

FedOpt is a federated optimization mechanism that was recently proposed to compress the communication stream by using a Sparse Compression Algorithm for communication efficiency and it integrates homomorphic encryption with differential privacy to prevent data leakage[94]. Another approach, named PCFL, was developed for federated AI in IoT[95]. This solution consists of a gradient spatial sparsification mechanism, a bidirectional compression system, and a secret sharing mechanism with lightweight homomorphic encryption.

Both solutions obtain high communication efficiency when compared to other approaches, however they are not suitable for federated AI models based on complex neural networks and high dimensional data.

ARCADIAN-IoT will develop a dependable and privacy preserving federated classifier. Data balancing solutions from centralized learning will be adapted and transferred to the federated setting and data imbalance will be considered in federated learning. Source and data integrity will be ensured in models.

3.7.1.3 Requirements

Requirement 6.1.1 – Malicious behaviors from sharing entities to be detected
When an entity collaborating in the federated learning process misbehaves during the protocol, it should be detected in order to invalidate the output
Related to Use Case Domain / Category / ID / Name
Domain A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure

[91] Duan, Moming et al. “Astraea: Self-balancing Federated Learning for Improving Classification Accuracy of Mobile Deep Learning Applications”, 2019 IEEE 37th Internal Conference on Computer Design.
[92] Zhao, Yue, et al. "Federated learning with non-iid data." arXiv preprint arXiv:1806.00582 (2018).
[93] Gao, Yansong, et al. "End-to-end evaluation of federated learning and split learning for internet of things." arXiv preprint arXiv:2003.13376 (2020).
[94] Li, Tian et al. “Federated Optimization in Heterogeneous Networks”, Proceedings of the 3rd MLSys, 2020.
[95] Fang, Chen, et al. "Privacy-preserving and communication-efficient federated learning in Internet of Things." Computers & Security 103 (2021): 102199.

Requirement preconditions
Multiple entities collaborate in sharing threat data
Requirement postconditions
The federated learning process is interrupted
Requirement Priority
Good to have

Requirement 6.1.2 – Local ML model to be lightweight
The models that are generated locally by the CTI should be lightweight, this will make the federated learning more efficient in the federated model computation
Related to Use Case Domain / Category / ID / Name
Domain A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
Threat data are available to train the federated model
Requirement postconditions
The trained model is used for the threat identification
Requirement Priority
Good to have

Requirement 6.1.3 – At least three heterogeneous devices/entities to be involved in the federated training
The federated AI mechanisms should support the training among at least three heterogeneous devices and entities
Related to Use Case Domain / Category / ID / Name
Domain A and C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
Devices/entities have threat data to share
Requirement postconditions
The trained model is used for the threat identification

Requirement Priority
Good to have

3.7.1.4 Evaluation KPIs

The federated AI module will be evaluated against the following KPIs:

1) Number of IoT devices/entities supported.
2) Time of training a federated learning model.
3) Size of the federated learning model.
4) Accuracy of federated learning model.
5) Computational complexity of federated learning model.
6) Robustness of federated learning model.

3.8 RECOVERY Vertical Layer

3.8.1 Self-Recovery

3.8.1.1 Summary

Self-Recovery mechanism will enable fast recovery of data and services after incidents. There are two crucial steps in the recovery phase – the recovery of credentials and the recovery of data and services. Both steps will be enabled by advanced cryptographic algorithms like functional encryption and secure multi-party computation if needed. To enable a full and fast recovery, the encrypted backups will be provided. Different keys will be distributed by which different levels of data will be able to be decrypted. For example, system administrators and incident response teams might get keys that enable different levels of decryption.

3.8.1.2 State of the Art

The component will pair the traditional recovery techniques with advanced cryptographic techniques. Different subjects will receive different cryptographic (functional encryption) keys and will be able to decrypt only the data that they have the rights to work on. This approach will make the backups safe and will simplify the process of recovery management. Furthermore, the techniques like secure multi-party computation will enable to aggregate different values of the encrypted data and backup only the aggregated values – the user of ARCADIAN-IoT will be able to specify the level of backup and by backing up only the aggregated values the backup will be cheaper (in the terms of the storage space) and faster. Secure multi-party computation will thus enable to back up the aggregated values from the files without seeing the files in the clear. To the best of our knowledge, no frameworks allow flexibility of recovery mechanisms to that extent. By other side the recovery systems need to be automated and ready to start on received notification. Therefore, we envision to prepare recovery scripts templates applicable to the ARCADIAN requirements. The scripts should take care of data recovery and in some cases starting the processes.

3.8.1.3 Requirements

Requirement 7.1.1 – Recovery mechanism
Each recovery system requires first an organised and detailed description of a running system. On second step we need to collect all data, that define a targeted system or process and all processes that are needed to set a system in an operational state. From the resource aspect, the recovery system needs the access to the data required for recovery, set of scripts that set up the processes and the machine which can run the recovery process and has access to the services and/or infrastructure that require recovery (network connectivity, etc).
Related to Use Case Domain / Category / ID / Name
Domain A and B
Requirements Scope (Person/IoT/Apps Services)
Infrastructure, Apps, IoT devices
Requirement preconditions
New infrastructure or affected device/process that needs the recovery. A recovery process triggered.
Requirement postconditions
IoT device/process recovered and functional.
Requirement Priority
Mandatory

3.8.1.4 Evaluation KPIs

The recovery process is successful if the application/process/IoT device is running as expected.

3.8.2 Credentials Recovery

3.8.2.1 Summary

The credentials recovery component will provide an automated recovery of the credentials after incidents for example a user's mobile was lost or stolen or a device was corrupted.

There are two levels of credential recovery applicable for the Self-Sovereign Identity solution as follows:

1) Recovery of the Decentralised Identifier (DID) and re-establishment of keys.

2) Recover of Verifiable Credentials issued to a wallet.

3.8.2.2 State of the Art

DID Recovery

The W3C DID specification[96] provides for one or more controllers that can carry out DID Management functions. *This is particularly important for key recovery in the case of cryptographic key loss, where the DID subject no longer has access to their keys, or key compromise, where the DID controller's trusted third parties need to override malicious activity by an attacker.* This capability will help to recover control of a DID for any scenario by being able to update the key by the identity owner or authorised delegate controller.

Whatever technology is used to provide the DIDs e.g., blockchain, sidetree with or without blockchain, or another DLT, a Decentralized Key Management System (DKMS) is the State of the Art enabler that *addresses what keys are needed, how they are used, where they should be stored and protected, how long they should live, and how they are revoked and/or recovered when lost or compromised* [8].

Independent of the lower layer implementing the DIDs there should be an operation to support the DKMS functions for recovery and update functions. Concerning the former, a DID Recovery operation would make use of a Recovery Key pair for which there must be a very strong safeguarding as compromised DID controller keys would not permanently result in a user losing control of a DID, whereas the compromise of a Recovery key would.

It is assumed the private key cannot be retrieved from a Trusted Execution Environment (TEE) in the device and thus cannot be backed up itself and so the DID authentication private public key generation and update will need to be part of the recovery process.

Verifiable Credentials Recovery

In order to recover Verifiable Credentials, it is needed to first perform a backup and therefore any solution should employ an encrypted backup option to local device or backup server. If backup is to a local device then this would be recommended to be done with a recovery key or if to a backup server then this is recommended to make use of DID authentication to prove they are the owner of the DID to get access to the VC backup, with no need of recovery key.

Once a wallet or agent has been recovered the Verifiable Credentials recovery can take place to recover the credentials.

In the case that control of the DID was not able to be recovered the VCs would have to be revoked and issued once more to the new wallet instance.

[96] https://www.w3.org/TR/did-core/

Network credentials recovery

In the case of loss of network credentials (like loss of cell phone) the current credentials recovery process is for the user to ask for a SIM swap.[97]

In a SIM swap the provider cancels the lost SIM and attaches the user's phone number to a new SIM, with new network credentials. It is important to perform a thorough identity check when a user asks for a SIM swap due to SIM swap attacks. In a SIM swap attack the attacker is able to perform a SIM swap on a SIM card owned by someone else. This locks the legitimate owner of the SIM of using it and gives the attack control over the victim's phone number, this can be used to crack 2FA systems that use SMS messages to confirm a user's identity. Any effort in automatizing this process should take this into account.

3.8.2.3 Requirements

Requirement 7.2.1 – Credentials recovery mechanism
Description: To recover lost, compromised or corrupted credentials for an SSI Agent or Wallet. Recover as well network credentials from network operator for authenticating devices/persons in third parties.
Related to Use Case Domain / Category / ID / Name
Domain A: A18, A19 *Domain B: B5* *Domain C: C11, C12, C13*
Requirements Scope (Person/IoT/Apps Services)
N/A
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.8.2.4 Evaluation KPIs

1) Number of DID Recovery operations.
2) Number of VC Recovery operations.
3) Successful processes for recovery of network credentials after security/privacy incidents.

[97] https://www.gsma.com/security/mobile-device-theft/

4) Support selective recovery ability in encryption mechanisms: who and what can be recovered.

3.9 SECURITY Horizontal Layer (crossing RECOVERY Vertical Layer)

3.9.1 Self-Healing

3.9.1.1 Summary

Self-healing is desired to mitigate the potential impact of a cyberattack against when protection rules for that kind of cyber-attacks are not installed in the system (e.g., Firewall rules not installed) and thus the attack has the potential to penetrate into the concerned IoT infrastructure. To this end, the Self-healing component in ARCANDIAN-IoT will be based on an autonomous loop, including the following subcomponent. First, the sensing and detection capabilities of a cyberattack such as Distributed Denial of Service (DDoS) provided by the **Flow Monitoring component.** This will allow to detect the cyber-attack. Second, the subcomponent Resource Inventory Agent (RIA) in charge of performing the periodical report of the IoT network infrastructure with the intention to allow an effective self-healing decision-making process using the topological information. Third, the subcomponent, Self-Healing Decision Maker (SHDM) will be in charge of determine what is the best plan to heal the network against that type of cyberattack, including advance intelligence aspect related to the device on where to stop the attack, the interface inside of such device and the sense of the communication flow passing for such interface, to inform about what is the best effective way to perform the healing of the network and also to send such information to the associated self-protection component. Finally, the fourth component is the **Self-Protection component** (and its associated sub-components explained later on) that will be in charge to perform the mitigation of the attack, and finally deploying the necessary counter-measures to enforce the mitigation actions (e.g., traffic blocking/dropping, traffic mirroring etc.).

3.9.1.2 State of the Art

The closest state of the art associated to the Self-Healing component is an Intrusion Prevention System that will perform autonomous inspection of traffic and enforcing of rules to heal and protect the network if there is a cyber-attack. Problems with these tools and thus the innovations address in this component are: I) They are traditionally designed for pure IP networks and thus they do not provide support for overlay networks nor for IoT network protection. 2) They are usually installed in a component, which is deployed in the middle of the data path and this is the only security control point available in the infrastructure and thus they do not provide support for dynamic distributed enforcing of protection/healing policies. 3) They do not understand the network topology and thus are not able to take plans based on such topologies, especially the topology of IoT networks.

3.9.1.3 Requirements

The requirements related to Flow Monitoring and Self-protection are indicated in their respective sections. These components are being used by the self-healing component and here only the requirements associated to other subcomponents only used in this self-healing component are indicated.

Requirement 8.1.1 – Distributed Healing

The self-healing component will be able to perform protection/healing rules in a distributed way according to the topological information gathered from the infrastructure with the main intention to heal/protect the network against DDoS attacks.
Related to Use Case Domain / Category / ID / Name
Domain C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
Attack already launched and protection rules not installed yet
Requirement postconditions
Attack Mitigated
Requirement Priority
Mandatory

3.9.1.4 Evaluation KPIs

The KPIs related to Flow Monitoring and Self-protection are indicated in their respective sections. These components are being used by the self-healing component and here only the KPIs associated to other subcomponents only used in this self-healing component are indicated. The self-healing component will be evaluation against the following KPIs:

1) Reaction time to heal a network according to the number of attackers launching an attack (Spatial Size).

2) Reaction time to heal a network according to the size/intensity of attackers from every attacker (Density).

3) Number of different network segments where the self-healing component can be installed (Flexibility).

4) Number of overlay protocols, the self-healing component can provide protection over (IoT Support).

3.9.2 Self-Protection

3.9.2.1 Summary

The IoT Infrastructure Self-protection component deals with continuous self-management of the enforcing of network protection policies in charge of protecting from cyberattacks against IoT network infrastructure through a continuous autonomous control loop in charge of achieving scalability in dealing with customized protection policies is large-scale IoT networks. To do so, the self-protection component will take control of the data path and perform a smart policy management algorithm to allow a high-scalable number of policies to be enforced into the IoT networks to protect against cyberattacks. The self-protection component is composed in 3 different subcomponents. First, the UWS OpenVSwitch Protection Decider will enforce the protection policies into the data path to achieve an effective protection. Second, the UWS

OpenVSwitch Data Path Security Controller will deal with all the policies loaded into the system and perform a continuous autonomous control loop to determine the subset of policies that should be installed into the kernel space in a given moment. And third, the Protection Control Agent (PCA) will be in charge of exposing an Intent-based API to allow different self-protection implementations to be plugged into the system.

The IoT Device Self-Protection component enforces protection policies and rules at device level. These policies include disabling malicious applications and preventing them to run or access data sensitive data in the device. This component also relies on information derived from other ARCADIAN-IoT components such as Behaviour Monitoring or Cyber Threat Intelligence (CTI).

3.9.2.2 State of the Art

Current firewalling protection mechanisms to enforce network protection policies are traditionally composed by algorithms that enforce a set of rules into the DataPath. These rules are checked in a sequential order against every packet that is trans versing the network. Our solution will provide an autonomous architecture in charge of loading a large-scale ruleset of policies and decided which subset will be enforced into the Datapath in a given time, avoiding the need to have all of them loaded at the same time. Also, the vast majority of firewalls, such as Cisco PIX, Watchdog, SonicWall, Barracuda Firewall, Juniper Firewalling, etc are providing capabilities for IP networks but however, suffer on providing support on IoT networks and this is where this component will provide innovation providing advance firewalling capabilities over this type of network.

The expansion of IoT devices and the increased need to protect such a heterogeneous combination of devices turn the job of device self-protection mechanisms into a much more complex task. The IoT Device Self-Protection component should focus on protecting devices and applying appropriate data protection policies. Usually, a set of protection layers classify data and services being used or interacting with the device. In other cases, these solutions also rely on data access monitoring, permission control or access control mechanisms.

ARCADIAN-IoT Device Self-protection component will be based on the aforementioned aspects and further enhanced into an autonomous self-protection solution applicable to different devices under various domains. Additionally, the intelligence gathered by other ARCADIAN-IoT components (e.g., Behaviour Monitoring or CTI) should further enhance the performance and effectiveness of the self-protection component.

3.9.2.3 Requirements

Requirement 8.2.1 – Mitigate Attack against IoT Overlay Networks
The control over the traffic should provide the definition of protection/mitigation rules of IoT network infrastructures.
Related to Use Case Domain / Category / ID / Name
Domain C
Requirements Scope (Person/IoT/Apps Services)
Infrastructure
Requirement preconditions
N/A
Requirement postconditions

Attack mitigated
Requirement Priority
Mandatory

Requirement 8.2.2 – Heartbeat monitoring mechanisms towards Arcadian-IoT framework should be implemented
The control over the traffic should provide the definition of protection/mitigation rules of IoT network infrastructures.
Related to Use Case Domain / Category / ID / Name
Domain A, C
Requirements Scope (Person/IoT/Apps Services)
Device
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 8.2.3 – Device should allow at least one type of adaptive settings (e.g., dynamic configuration, rule enforcement, permission granting/revoking)
The control over the traffic should provide the definition of protection/mitigation rules of IoT network infrastructures.
Related to Use Case Domain / Category / ID / Name
Domain A, C
Requirements Scope (Person/IoT/Apps Services)
Device
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 8.2.4 – Device should provide administrative privileges to self-protection component
The control over the traffic should provide the definition of protection/mitigation rules of IoT network infrastructures.
Related to Use Case Domain / Category / ID / Name
Domain A, C
Requirements Scope (Person/IoT/Apps Services)
Device
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 8.2.5 – Device should be able to periodically obtain up-to-date classification of applications and services (e.g., from reputation system or CTI)
The control over the traffic should provide the definition of protection/mitigation rules of IoT network infrastructures.
Related to Use Case Domain / Category / ID / Name
Domain A, C
Requirements Scope (Person/IoT/Apps Services)
Device
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.9.2.4 Evaluation KPIs

The self-protection component will be evaluated against the following KPIs:

1) Number of mitigation/protection rules that are able to be installed in the component.
2) Number of different network segments where the self-protection component can be installed (Flexibility).
3) Number of overlay protocols, the self-protection component can provide protection over (IoT Support).

The device self-protection component will be evaluated against the following KPIs:

1) Provide at least two self-protection mechanisms (e.g., policy change, rule enforcement) for the supported devices.
2) Support at least one self-protection mechanism (e.g., data encryption, policy change, rule enforcement) for scenarios with no connectivity.

3.10 COMMON Horizontal Layer (crossing RECOVERY Vertical Layer

3.10.1 Permissioned blockchain

3.10.1.1 Summary

In ARCADIAN-IoT a blockchain is needed for rooting the trust for the Decentralised Identifiers which are covered in section 3.1.1. As such a main objective of the project is to implement a permissioned blockchain that would be based on open-source alternatives such as Hyperledger Fabric, Quorum or Hyperledger Besu.

The permissioned blockchain is one of the horizontal components that will be part of the ARCADIAN-IoT framework, providing its immutable auditability and traceability properties to the data under management. Given the sensitive nature of data that will be shared in the network, ARCADIAN-IoT will use a private permissioned blockchain approach. Private permissioned blockchains place restrictions on who is allowed to participate in the network and in what transactions. It can have several conditional access features for users to obtain permission to operate at given levels. In order to interact with the blockchain, software clients typically run their own node, automatically updating the common state internally and then notifying the rest of nodes. Importantly the permissioned blockchain has much higher throughput and aimed more at enterprise solutions whereas the public permissionless blockchains are much slower due to their global participation and complex consensus proofs.

3.10.1.2 State of the Art

Decentralised Identifiers may be used as identifiers for users´ wallets or issuer and verifier organisations´ agents and as such they can reside on mobile smartphones and organisations´ servers, for the end users that interact with IoT services and apps. However, also in scope of the project is the possibility to provision IoT devices or their proxy gateways, with Decentralised Identifiers noting that this is a major challenge for devices that typically have constrained MCUs.

Time has not stood still, in the Self-Sovereign Identity sector where the blockchain was first employed to root the trust of each DID in a specific transaction on the decentralised ledger with

all the benefits that it brings with not relying on a central authority. Since then DIF[98] has developed the Sidetree 1.0.0 specification (published in 2021) that provides a distributed file system in which it anchors its trust with hashes in a merkle tree structure on a blockchain, with the advantage that it can now handle hundreds or thousands of batched DID transactions in one operation on the blockchain. DIF have also been working on the universal DID resolver[99] and this is compatible with Sidetree implementation to find the DID Doc on the distributed file system from first interrogating the blockchain. The result is that the provision and handling of DIDs can now be provided by Sidetree which is blockchain agnostic and is provided at much reduced costs, higher throughput improved scalability but is still crucially anchored on a blockchain. Microsoft led the development of the open source Sidetree implementation as part of its development of the open-source ION DID Method implementation on Sidetree anchored on Bitcoin.

We see ION is anchored on a public blockchain so if Sidetree is to be employed in ARCADIAN-IoT it should be on a permissioned blockchain so to control access to who can write and access it as previously specified. Some such OS implementations are starting to emerge such as that of Sidetree with Hyperledger Fabric ledger backing[100].

IOTA has also been very active in the decentralised identity space and are developing the IOTA Identity framework to implement common standards for Decentralized Identity in both a DLT agnostic and iota method specification1[101]. The IOTA method is anchored on their implementation of a ledger technology called Tangle[102] and provides a free to use permissionless ledger similar to blockchain but based on directed acyclic graph (DAG). They are developing the framework and client components on top of RUST which enables to compile without the filesystem or other OS facilities, and thus is more suited to be deployed on IoT devices with constrained microcontrollers that don´t have an Operating System. Upon initial examination the IOTA ledger does not fit the requirements of the project to implement a permissioned blockchain, but at the same it is providing a whole identity ecosystem that will support it but also intends to be ledger agnostic with development of common protocols such as DIDCOMM[103].

Both the Sidetree anchored on a permissionless blockchain and the IOTA Tangle approaches should be taken into consideration when proposing the final solution.

3.10.1.3 Requirements

Requirement 9.1.1 – Provide a permissioned blockchain
Description: To provide a permissioned blockchain to anchor the trust for Distributed identities.
Related to Use Case Domain / Category / ID / Name
(Use Case Domain / Category / ID / Name) *A1, A2, A7* *B1, B3, B4, B6* *C1, C2, C4, C5, C7*
Requirements Scope (Person/IoT/Apps Services)

98 https://identity.foundation/

99 https://github.com/decentralized-identity/universal-resolver
100 https://github.com/trustbloc/sidetree-fabric
101 https://github.com/iotaledger/identity.rs
102 https://github.com/TangleID/TangleID/blob/develop/did-method-spec.md
103 https://identity.foundation/didcomm-messaging/spec/

(*Person/IoT/Apps Services)*
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.10.1.4 Evaluation KPIs

KPIs related to the blockchain implementation are related to the DID method operations and as such the following KPIs are specified:

Operations:

- Create.
- Update.
- Deactivate.
- Recover.

3.11 LEGAL DATA PROTECTION REQUIREMENTS (E-LEX)

3.11.1 Summary

ARCADIAN-IoT project involves the use of different types of personal data. This raises numerous data protection issues and potential challenges need to be assessed and addressed. In particular, the use of technological components such as blockchain, AI, biometric technologies and drones could raise concerns on data privacy, data protection, digital identities and data ethics. Therefore, in achieving the goals of ARCADIAN-IoT Project, a transparent ecosystem for personal data protection, supporting the pillars of the EU's General Data Protection Regulation ("GDPR"), should be developed. Some of these issues, actually, were already the subject of attention of the different partners who, with reference to the various requirements, have already provided for measures aimed at the security of the components used and, therefore, of personal data processed. However, some issues still need to be addressed and requirements must be identified. Since the requirements for the implementation of the different components are not uniform, this section provides a separate analysis of the different technologies used within ARCADIAN-IoT project that may present risks in relation to the provisions of the GDPR, providing the relative requirements for each.

3.11.2 State of the Art

As mentioned in the previous paragraph, the research carried out within the ARCADIAN-IoT project involves the use of technological components which, in the same way, imply numerous issues in terms of protection of personal data.

3.11.2.1 Permissioned blockchain system

The use of a private permissioned blockchain system provides immutable auditability and traceability properties to the data under management. The permissioned blockchain consists of a special-purpose blockchain implementation that only works within the ARCADIAN-IoT systems.

It will be permissioned, meaning that instead of a proof-of-work or proof-of-stake consensus, a central authority will provide the permission to participate in the ARCADIAN-IoT blockchain network. The goal of including an implementation based on a blockchain platform is to provide secure and trustable means to operate. Indeed, it increases the confidence of European citizens in the operations on their personal data. The perception of control rises and the compliance of regulations - such as the GDPR - is greater. A permissioned blockchain network will ensure a secure and reliable identification, authentication and data access, acting as a distributed and secure means. On the other hand, 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 principles set out in the GDPR (e.g., the principle of data minimisation), as well as the rights that the GDPR grants to data subjects and which should always be exercisable by them.

3.11.2.2 Biometric technology

Components based on facial recognition technologies will also be used in research activities. As pointed out in the previous paragraphs, biometrics components will be able to identify persons through face recognition for identity management purposes. In order to identify the legal requirements to achieve in the implementation of this component, it should be noted that the facial recognition activity in question involves the processing of biometric data pursuant to the Article 4(1) no 14, GDPR, defines "biometric data" as any "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question". Then, biometric data fall within the special categories of personal data regulated by the Article 9, GDPR which states that "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" unless one of the conditions laid down in Article 9(2) is met and, in particular, if the data subject has given explicit consent or if the processing. Moreover, it should be noted that the processing of such types of data is also regulated by several guidelines, such as the "Working document on biometrics (WP80)" and the "Opinion 3/2012 on developments in biometric technologies" adopted by the Working Group Article 29, the "Guidelines 3/2019 on processing of personal data through video devices" and "Guidelines 02/2021 on Virtual Voice Assistants" published by the European Data Protection Board, as well as the "Guidelines on Facial Recognition" adopted by the Consultative Committee of the Convention 108. Integrating facial recognition technologies to existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data, since the uses of these technologies do not always require the awareness or cooperation of the individuals whose biometric data is processed.

3.11.2.3 Anonymisation vs. Pseudonymisation

As mentioned above, many of the risks related to the use of personal data have already been addressed by the partners, who intend to develop the management of privacy and data in general. One of these measures is, where applicable, pseudonymisation or, if possible, anonymisation of data. Although similar, anonymisation and pseudonymisation are two distinct techniques that permit data controllers and processors to use de-identified data. The difference between the two techniques rests on whether the data subjects can be re-identified, in particular:

- Recital 26 of the GDPR defines anonymised data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable." When done properly, anonymisation places the processing and storage of personal data outside the scope of the GDPR;

- Article 4 (5) of the GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." By rendering data pseudonymous, controllers can benefit from "relaxed" standards, but do not fall outside the scope of the GDPR.

In conclusion, the use of said techniques allows greater data security but, in any case, presents certain risks of which Partners must be aware. The first, which seems trivial but is not, is linked to the fact that pseudonymisation and anonymisation are often overlapped concepts, thus risking treating as anonymous (and therefore without the guarantees of the GDPR) data that are only pseudonymised. The second, which relates specifically to pseudonymisation, concerns the management of the re-identifier.

3.11.2.4 Drones

The components that usually form a drone could not be in themselves capable of processing personal data of a subject, but a drone could anyway have a disruptive influence on the private life of individuals. The most common equipment of a drone are video cameras: the drone can acquire high resolution images, as well as being equipped with the camera's stabilisation feature, that consists in the possibility to improve the quality of an image, captured in sub-optimal conditions and that presents vibrations or interferences. These features permit reproducing an image of a person that can be recognised or identified, to follow, for example, someone's movements. Furthermore, drones are equipped with sensors, such as, gyroscope, barometer, accelerometer, GPS, etc. Thanks to these sensors, a drone can identify objects, vehicles and vessels, obtaining information on their position. The result is that these devices can, due to specific circumstances, endanger the protection of the fundamental rights of the individual, such as the respect for private and family life. In particular, the use of drones entails a number of privacy risks, including the processing of biometric data resulting from the use of highly innovative cams, on the one hand, and the processing of the location data of the data subjects, on the other. With reference to the risks underlying the recognition of an individual through his/her biometric data (captured, where appropriate, through the camera of a drone), please refer to what has been said about biometric technologies in the previous paragraph 3.11.2.2.

3.11.3 Requirements

3.11.3.1 Requirements for component using blockchain technology

Requirement 10.1 – Ensure the exercise of data subject's rights
With reference to components using blockchain technology, it is necessary to ensure that the citizens can exercise the data subject rights according to the GDPR, giving back the control to the data subject by letting her/him the choice to "remember" or "forget" their identifiers, in order to be compliant with GDPR and, in particular, to the "right to be forgotten" when the user stop using services (or upon request).
Related to Use Case Domain / Category / ID / Name
All
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)

Requirement 10.2 – Comply with GDPR's principles
According to the purpose specification principle, personal data must only be collected for specified, explicit and legitimate purposes, while the compatible use condition and the minimisation principle require personal data not to be further processed in a way incompatible with those purposes. In the case of blockchain technology, the problem arises because, once added to the database, the data will always continue to be processed. Data controllers relying on blockchain technology should therefore clearly communicate to data subjects that they are using this technology and explain the related implications, such as the fact that the processing is not limited to the original operations. Furthermore, the possibility to update and rectify the data (in compliance with the principle of accuracy of the data) should be foreseen, as well as, once the purpose has been achieved, to delete the data in the light of the principle of limited storage. It is also worth remembering that the GDPR only applies to personal data: this implies that where data continues to be processed beyond its initial purpose, but only in an anonymised form, then this processing no longer falls within the scope of the GDPR. Therefore, another requirement could be the anonymisation of the data in such cases.
Related to Use Case Domain / Category / ID / Name
All
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.11.3.2 Requirements for biometric components

Requirement 10.3 – Accuracy of data used
With reference to all the personal data processed and, in particular, to biometric data used for facial recognition purposes, it is necessary to take steps to ensure that facial recognition data are accurate. This can be achieved by testing systems, as well as identifying and eliminating disparities with regard to demographic variations in skin colour, age and gender and, thus, avoiding unintended discrimination. Furthermore, according to aforementioned Guidelines of the Convention 108, back-up procedures should be provided for in case of system failure if the physical characteristics do not correspond to the technical standards.
Related to Use Case Domain / Category / ID / Name
A
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 10.4 – Renewal of data and reliability of the component
The facial recognition system requires periodic renewal of data in order to train and improve the algorithm used. Each algorithm has a percentage of recognition reliability, therefore should this reliability deteriorate, it will be necessary to renew the training photos. This requirement is also connected to the reliability of the component used (i.e., the effectiveness of the algorithm). Partners shall ensure the highest possible level of reliability, considering that the use of a facial recognition technology might result in very significant consequences for the individual.
Related to Use Case Domain / Category / ID / Name
A
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 10.5 – Awareness
While developing and using facial recognition technologies, it is necessary to take reasonable steps to help use them with transparency and respect for privacy. This goal shall be achieved by providing user-friendly privacy policies, easy-to-understand signage that indicates that a facial recognition technology is deployed in a specific space, etc.
Related to Use Case Domain / Category / ID / Name
A
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.11.3.3 Anonymisation and pseudonymisation requirements

Requirement 10.6 – Distinguish between the two techniques and manage the re-identifier properly
As mentioned, it is necessary to distinguish (and process differently) between anonymised and pseudonymised data: this depends, as said, on whether or not the data subject can be "traced" through other factors. If it is "reasonably likely" that data subjects can be re-identified, any additional information which, when combined, allows the data subject to be traced should be protected from unauthorised access, through the use of appropriate technical and organisational measures.
Related to Use Case Domain / Category / ID / Name
All
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.11.3.4 Requirements for drones

Requirement 10.7 – Proportionality, strict necessity and security
The use of drones involves the collection and processing of a considerable amount of personal data. Although European case law and legislation does not preclude such uses of personal information where it is limited to specific circumstances and circumscribed purposes, that need to be analysed and identified. Moreover, attention should be paid to the strengthening of security (both physical and cyber).
Related to Use Case Domain / Category / ID / Name
A
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

Requirement 10.8 – Awareness and control over data
Since, as mentioned above, among the components of a drone there are technologies (such as GPS) allowing the localisation of the data subject, the latter should be properly informed of this circumstance and should give his/her consent to such processing. Therefore, in the implementation of such a component, appropriate documentation should be foreseen in order to provide data subjects with the necessary information to understand the processing carried out and to give properly informed consent. Furthermore, from a technical point of view, the system should be built in such a way that the data subject can easily stop the tracking of his/her location.
Related to Use Case Domain / Category / ID / Name
A
Requirements Scope (Person/IoT/Apps Services)
Person (Data Subject)
Requirement preconditions
N/A
Requirement postconditions
N/A
Requirement Priority
Mandatory

3.11.4 Evaluation KPIs

1) Carrying out a data protection impact assessment (DPIA) before and during the implementation of components in any case it is requested by the GDPR.
2) Adopt appropriate security measures pursuant to Article 32 of the GDPR.

4 CONCLUSIONS

This document captures and describes the ARCADIAN-IoT framework requirements gathered during the analysis made regarding distributed, dynamic and automated trust management and recovery solutions, with approaches to manage the identity of persons and objects, including self-encryption/decryption schemes with recovery ability to be performed.

This document represents deliverable D2.4, being the outcome of Task T2.2, and will also serve as input to the research to be performed in WP3 and WP4, that will also allow the assessment of the project iteratively in WP5.

This study was combined with the outcomes of Task 2.1, which interactively identified which ARCADIAN-IoT components characteristics were required to meet the use cases' needs, aligned with the project objectives. The output of this report is also contributing to the architecture specification in Task 2.3, and launching the work of WP3 and WP4.

The result is a set of 52 technical requirements spread among 20 components and 6 layers, and also 8 regulatory/legal requirements. This set is assessed, justified, and considered relevant, coherent, and complete. All the listed requirements are related to the components of the ARCADIAN-IoT platform, applicable at least to one of the use cases, and therefore relevant for the project demonstration and validation.

Each requirement was evaluated to its priority, to help the team planning their implementation in different phases of the prototype deployment.

Although this set of requirements is considered as definitive towards the project objectives, the resultant implementation is following an agile approach, which can lead to adjustments, changes and/or improvements to the requirements, while the architecture is being defined and work is ongoing, right until the end of the project.

REFERENCES

1. EC, *European Self-Sovereign Identity Framework*, Website https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=379913698, retrieved 13 Oct 2021
2. EC, *Commission proposes a trusted and secure Digital Identity for all Europeans*, Website, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663, retrieved 13 Oct 2021
3. Soltani, Reza, (2021), *A Survey of Self-Sovereign Identity Ecosystem*, https://www.hindawi.com/journals/scn/2021/8873429/, retrieved 13 Oct 2021
4. https://www.hyperledger.org/, Website, retrieved 13 Oct 2021
5. https://www.hyperledger.org/use/aries, Website, retrieved 13 Oct 2021
6. DIF-Decentralized Identity Foundation, 2021, https://identity.foundation/, Website, retrieved 13 Oct 2021
7. W3C Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/#did-controller, website, retrieved 19 Oct 2021
8. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0051-dkms/dkms-v4.md, website, retrieved 19 Oct 2021
9. Sidetree Specification 1.0.0, https://identity.foundation/sidetree/spec/, website, 19 Oct 2021
10. DIF Universal Resolver, https://dev.uniresolver.io/, website, retrieved 19 Oct 2021
11. Sidetree OS Implementation, https://github.com/decentralized-identity/sidetree, retrieved 19 Oct 2021
12. ION OS Implementation, https://github.com/decentralized-identity/ion, website, retrieved 19 Oct 2021
13. Sidetree Fabric OS implementation, https://github.com/trustbloc/sidetree-fabric, retrieved 19 Oct 2021
14. IOTA Unified identity, https://files.iota.org/comms/IOTA_The_Case_for_a_Unified_Identity.pdf, website, retrieved 20 Oct 2021
15. IOTA Identity Framework Guide, https://wiki.iota.org/identity.rs/introduction, website, retrieved 20 Oct 2021
16. IOTA Identity for Tangle, https://github.com/iotaledger/identity.rs, website, retrieved 20 Oct 2021
17. RUST, https://www.rust-lang.org/what/embedded, website, retrieved 20 Oct 2021
18. Tangle, iota1_4_3.pdf (ctfassets.net), https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf, website, retrieved 20 Oct 2021
19. DIF DIDCOMM Specification, https://identity.foundation/didcomm-messaging/spec/, Website, retrieved 20 Oct 2021
20. IOTA ecosystem components, https://github.com/iotaledger, Website, retrieved 20 Oct 2021
21. Author Surname, First name initials, (Year of Publication or most recent Update), *Website/Article Title, Website URL, Date of access.* (For Websites, e.g. Cain, A., & Burris, M. (1999). *Investigation of the use of mobile phones while driving*, http://www.cutr.eng.usf.edu/its/mobile_phone_text.htm, retrieved January 15, 2000.)