Grant Agreement N°: 101020259

Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D6.4: Standardization activities report

Work package	WP6
Task	Task 6.3
Due date	10/04/2023
Submission date	28/04/2023
Deliverable lead	Truphone
Version	2.0

Abstract

This public report constitutes the deliverable D6.4 of ARCADIAN-IoT, a Horizon 2020 project with **grant agreement number 101020259**, under the topic **SU-DS02-2020**. The main purpose of this document is to present the current ARCADIAN-IoT standardization initiatives. The work was carried out as part of **Task 6.3 (Standardization contribution)** and has considered inputs from the technical and integration tasks of the work packages WP2, WP3, WP4 and WP5. Truphone (TRU) is coordinating the effort of this task, which has the participation of Instituto Pedro Nunes (IPN) and of RISE Research Institutes of Sweden (RISE). This is an intermediary report, which will have an updated final version in the last month of the project (April 2024). For the time being, the involved partners have identified the relevant standardization bodies and industry fora to contribute to, are regularly participating in the meetings of the relevant Working Groups therein, carried out several community awareness actions, and made some initial contributions with the preliminary knowledge and results that stem from ARCADIAN-IoT.

Keywords: ARCADIAN-IoT standardization contributions; Cybersecurity standardization; IETF RATS; IETF SCHC; IETF CoRE; GSMA IoT SAFE, GSMA eSIM.

Document Revision History

Version	Date	Description of change	List of contributors
V0.1	08/09/2022	- Document structure	TRU (editor), IPN, RISE
V0.9	31/03/2023	- First complete draft	TRU (editor), IPN, RISE
V1.0	10/04/2023	- Complete version ready for internal and Security Advisory Board (SAB) review	TRU (editor), IPN, RISE
V1.0r	17/04/2023	- Version including internal revision comments	RISE
V2.0	24/04/2023	- Final version, considering internal and SAB review	TRU (editor), IPN, RISE

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 targets the standardization efforts made in ARCADIAN-IoT. Considering that the project focuses on a framework for trust, security, and privacy management for the IoT, there are several Standards Development Organizations (SDOs) and industry fora that are relevant to feed the research and that can benefit of the outcomes of the project, strengthening the technical specifications or obtaining insights and feedback about the technical directions to pursue. While the consortium is aware of the most relevant SDOs, the standardization efforts have targeted the IETF and GSMA Working Groups that directly relate with ARCADIAN-IoT and that are of partners' interest for result exploitation. Particularly, in the IEFT, ARCADIAN-IoT partners have focused on the Working Groups RATS, CoRE and SCHC, and, in GSMA, while closely accompanying the Working Groups eSIM and SAM, the work targeted the IoT SAFE community. Currently, ARCADIAN-IoT is regularly present in these Working Groups' meetings and has already carried out several community awareness actions. While some relevant contributions were already made, the standardization inputs will continue until the end of the project using for such the project results.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **5**
TABLE OF CONTENTS **6**
LIST OF FIGURES **7**
ABBREVIATIONS **8**
1. INTRODUCTION **11**
2. OBJECTIVES AND APPROACH **12**
2.1. Objectives 12
2.2. Contribution types 12
2.3. Approach 14
3. TARGET STANDARDIZATION BODIES AND INDUSTRY FORA **16**
3.1. Standardization bodies and industry fora relevant for ARCADIAN-IoT 16
3.2. IETF 19
3.3. GSMA 22
4. STANDARDIZATION ACTIVITIES AND CONTRIBUTIONS **25**
4.1. IETF – RATS WG 25
4.2. IETF – CoRE and SCHC WG 26
4.3. GSMA – IoT SAFE 28
4.4. GSMA – eSIM and SAM WGs 32
4.5. Overall summary of current contributions to IETF and GSMA 33
5. NEXT ACTIVITIES PLAN **34**
5.1. IETF 34
5.2. GSMA 35
6. CONCLUSIONS **36**

LIST OF FIGURES

Figure 1 - ARCADIAN-IoT Framework 11
Figure 2 - ARCADIAN-IoT's approach to contribute to standardization 15
Figure 3- The GSMA in numbers[17] 23
Figure 4 - GSMA IoT SAFE components and overall architecture 29
Figure 5 - Head of R&D of TRU, presents at TADSummit 2022 31
Figure 6 - ARCADIAN-IoT preliminary results in GSMA IoT SAFE plenary meeting 32
Figure 7 - Overall summary of current contributions to IETF and GSMA 34

ABBREVIATIONS

4G	Fourth-generation technology standard for broadband cellular networks
5G	Fifth-generation technology standard for broadband cellular networks
ABE	Attribute-based encryption
ACE	Authentication and Authorization for Constrained Environments
AI	Artificial Intelligence
ART	Applications and Real-Time Area
CBOR	Concise Binary Object Representation
CoRE	Constrained RESTful Environments
CoAP	Constrained Application Protocol
COSE	CBOR Object Signing and Encryption
CSIRT	Computer Emergency Response Team
CWT	CBOR Web Token
DICE	DTLS in Constrained Environments
DID	Decentralized Identifiers
DRIP	Drone Remote ID Protocol
DTLS	Datagram Transport Layer Security
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
ETSI	European Telecommunications Standards Institute
FIDO	Fast Identity Online
GSMA	Global System for Mobile Communications Association
HTTP	Hypertext Transfer Protocol
HW	Hardware
iSIM	Integrated Subscriber Identity Module
IAB	Internet Architecture Board
ICT	Information and Communications Technology
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet of Things

IoT SAFE	IoT SIM Applet For Secure End-to-End Communication
IOTOPS	IoT Operations
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISOC	Internet Society
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
LAKE	Lightweight Authenticated Key Exchange
LoRa	Long Range
LPWA	Low-Power Wide-Area
LPWAN	Low-Power Wide-Area Network
M2M	Machine-to-Machine
MNO	Mobile Network Operator
MSP	Middlebox Security Protocol
MVNO	Mobile Virtual Network Operator
MWC	Mobile World Congress
NB-IoT	Narrowband IoT
OAuth	Open Authorization
OSCORE	Object Security for Constrained RESTful Environments
PSA	Platform Security Architecture
RATS	Remote Attestation Procedures
REST	Representational State Transfer
RFC	Request For Comments
RoT	Root of Trust
SAM	Secured Applications for Mobile
SAS	Security Accreditation Scheme
SCHC	Static Context Header Compression
SDO	Standards Development Organization
SIM	Subscriber Identity Module
SUIT	Software Updates for Internet of Things
TAD	Telecommunication Applications Developers
TC	Technical Committee

TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TEEP	Trusted Execution Environment Provisioning
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UN	United Nations
W3C	World Wide Web Consortium
WI-SUN	Wireless Smart Utility Network
WG	Working Group

1. INTRODUCTION

The Internet of Things (IoT) is assuming a prominent role in current and future digitisation of society. The potential related with the monitoring and management of *things* over the Internet enables the optimization of existing services, generates new business opportunities, and creates new digital experiences for people. In 2030, it is expected to have more than 29 billion connected devices[1], i.e., more than 3 devices connected to the Internet per person. In this context, cybersecurity is a key factor that determines the success or failure of IoT solutions. Products that rely on connected devices that are vulnerable, leak confidential data, or are prone to be controlled by unauthorized agents are likely to fail due to serious brand damages and legal sanctions. In this sense, ARCADIAN-IoT (Figure 1) proposes a comprehensive framework for security, trust and privacy management for IoT, where solution providers have at their disposal a set of features that allow to make their IoT ecosystems less vulnerable and more resilient to attacks, and more able to efficiently respond to cyber incidents.

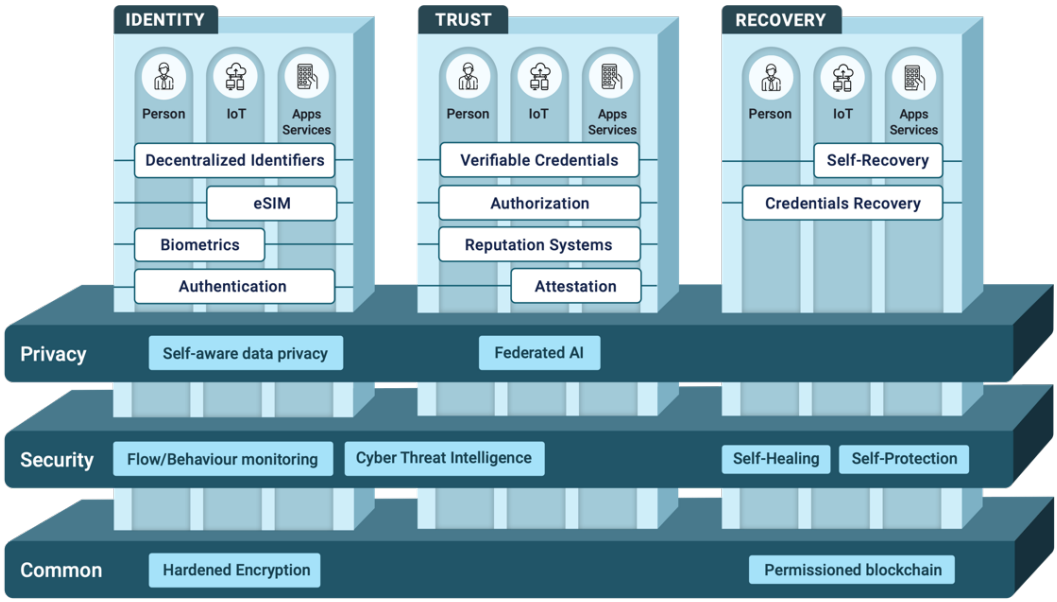

Figure 1 - ARCADIAN-IoT Framework

Considering the cybersecurity focus, and the objective of the framework to be holistic to the IoT domain, the use of standards and the contribution to standardization with the research results is

[1]https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

quite relevant and appropriate. ISO defines a standard as "the best way of doing something"[2], being the "distilled wisdom of people with expertise in their subject matter". Particularly in IT security, ISO define those standards as a way to "help keep sensitive information secure". Regarding the process of defining standards based on stakeholders' consensus, it is known as standardization[3]. In this process, the entities from a particular industry agree on the guidelines to be followed to build a well-accepted product or service. It aims to ensure uniformity, improve quality and safety, increase productivity and efficiency, and to attract customers with the trust that the best practices are being followed. Therefore, standardization has a close relation to the creation and evolution of products and services – those that follow well-accepted standards are likely to gather more trust from customers. Particularly in cybersecurity, organizations should use the related standards to implement appropriate measures to protect their systems and data from cyber attacks[4]. The compliance with standards can even be mandatory, when demanded to be enforced by laws or regulation (e.g., for health and safety reasons).

This report focuses on how ARCADIAN-IoT contributes to standards and to standardization processes that help build secure IoT products. The next section presents the project standardization objectives, the different types of contribution and the general approach followed to contribute to the target SDOs. Section 3 focuses on describing the target standardization bodies and industry fora. The specific standardization activities and contributions that already took place will be described in section 4. The final section describes the upcoming standardization activities and our preliminary drawn conclusions.

2. OBJECTIVES AND APPROACH

2.1. Objectives

ARCADIAN-IoT's first standardization objectives are to create community awareness at SDOs and industry fora relevant for the project, particularly those where the project results may have interest. For what regards new standardization contributions, the target defined at the beginning of the project was of 10 contributions to the process of standard definition.

2.2. Contribution types

To determine the potential types of standardization contribution, reference information from one of the most relevant SDOs, Internet Engineering Task Force (IETF), was considered. In its RFC

[2] https://www.iso.org/standards.html

[3] https://www.wallstreetmojo.com/standardization/

[4] https://www.itgovernanceusa.com/cybersecurity-standards

5378[5] (RFC stands for Request For Comments), IETF specifies the best practices, policies and rights for its community, namely with what concerns "Contributions to IETF". In the definitions section of this document, it is presented exactly what is, and what is not, considered a "Contribution" (section 1. a.):

> *c. "IETF Contribution": any submission to the IETF intended by the Contributor for publication as all or part of an Internet-Draft or RFC (except for RFC Editor Contributions described (...) below) and any statement made within the context of an IETF activity. Such statements include oral statements in IETF sessions as well as written and electronic communications made at any time or place, that are addressed to:*
>
> - *the IETF plenary session,*
> - *any IETF working group or portion thereof,*
> - *any Birds of a Feather (BOF) session*
> - *the IESG, or any member thereof on behalf of the IESG,*
> - *the IAB or any member thereof on behalf of the IAB,*
> - *any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,*
> - *the RFC Editor or the Internet-Drafts function (...).*
>
> *Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions (...).*

From this definition, it is possible to assume that the scope of contribution to the process of standard development (standardization) is broad, encompassing not only direct inputs to standard documents, but also statements made in the context of the work being addressed.

To further specify standardization contribution types, during the initial stage of ARCADIAN-IoT, we organized a session led by the Chair of the IETF CoRE Working Group. Most ARCADIAN-IoT's consortium partners participated in this session, which focused in topics like: reasons to do standardization; an overview of the IETF compared with other SDOs; the IETF organization, culture, document types and lifecycle; and how to contribute to the IETF. Particularly, the following types of contributions were highlighted:

- **Passive/lightweight engagement**:
  - Keep up to date with current activities and developments;
  - Keep reading documents as they are revised;
  - Keep following discussions at meetings and on mailing lists.

[5] https://www.rfc-editor.org/rfc/rfc5378

- **Active engagement**:
  - Provide comments/input to existing documents (e.g., in meetings or mailing lists);
  - Provide reviews to existing documents (e.g., through mailing lists);
  - Declare interest and support to an existing document.
- **Very active engagement**:
  - Be an author of Internet Drafts;
  - Provide SW implementations of an existing document and/or test results of the implementation of current specifications.

Considering the IETF a renowned SDO that has a clear and documented definition of standardization contribution, and the concrete inputs from the Chair of an IETF Working Group (speaking as an individual), the ARCADIAN-IoT consortium decided to measure its involvement in standardization activities in accordance with the above-mentioned types of contribution. Linking to the standardization objectives previously mentioned, for the 10 contributions defined as target at the beginning, we will consider the number of actions of Active or Very active engagement. The actions of Passive/lightweight engagement are understood as the ones needed to be able to perform the actions of Active or Very active engagement (which includes community awareness actions).

2.3. Approach

The approach to perform contributions to standardization is dependent on the contributor positioning in its SDOs of interest. Naturally, experienced contributors are already enrolled in the Working Groups of their SDOs of interest (if these need enrolment), know their processes and have established relations with other members. This is not the case for all the potential contributors, or for contribution of expert contributors in new Working Groups or new SDOs. In ARCADIAN-IoT, while all the partners that are contributing to standardization have some level of experience in the area, it was considered relevant to take a more holistic approach to the process.

The approach defined has an iterative nature and is depicted in Figure 2. Starting from ARCADIAN-IoT objectives (1) we defined the relevant standards, SDOs and SDOs Working Groups (which target specific standards or specifications); (2) The SDOs Working Groups considered to be relevant are those that are important to the project (according to its objectives) and that match the contributor expertise and their technology exploitation interests. Furthermore, we organized the overview about the IETF standardization process (1.1) described in the previous section. Having selected the SDOs' Working Groups of interest, each partner enrolled in those groups (if this action applies to that SDO) (3) and performed community awareness actions regarding the project, its objectives, and the relation with the standards targeted by their work (3.1). In this step, as previously defined, lightweight/passive engagement has already occurred, including getting up to date with the Working Group activities (e.g., by participating in the Working Groups' meetings). Active engagement has also occurred, including through the declaration of interest to support a particular specification/standard. The community awareness actions may also target technology communities to whom the standards are relevant, being this understood as a relevant contribution to SDOs activities as well. After being part of the group of

interest, some partners considered relevant to implement the standards specification (4), when appropriate according to ARCADIAN-IoT components' objectives. The standard technology implemented in each component was seen as the baseline for attempting to go beyond that state of the art. This action also prepared the partners to provide more concrete technical contributions to the targeted standards (e.g., to existing documents) (5), which, according to the definitions from the previous section, are actions denoting very active engagement (e.g., based on the sharing of implementations and results from testing the specifications). Each contribution also reinforced the partners' expertise in the standardization process (1.1), particularly to the specifically targeted SDO and Working Group. Also, through the interaction with other SDO' members, experts in ARCADIAN-IoT areas that are focused on the targeted Working Groups, and with the specifications' implementation, partners were able to better understand how to accomplish ARCADIAN-IoT objectives (1), closing the iterative loop shown in Figure 2.

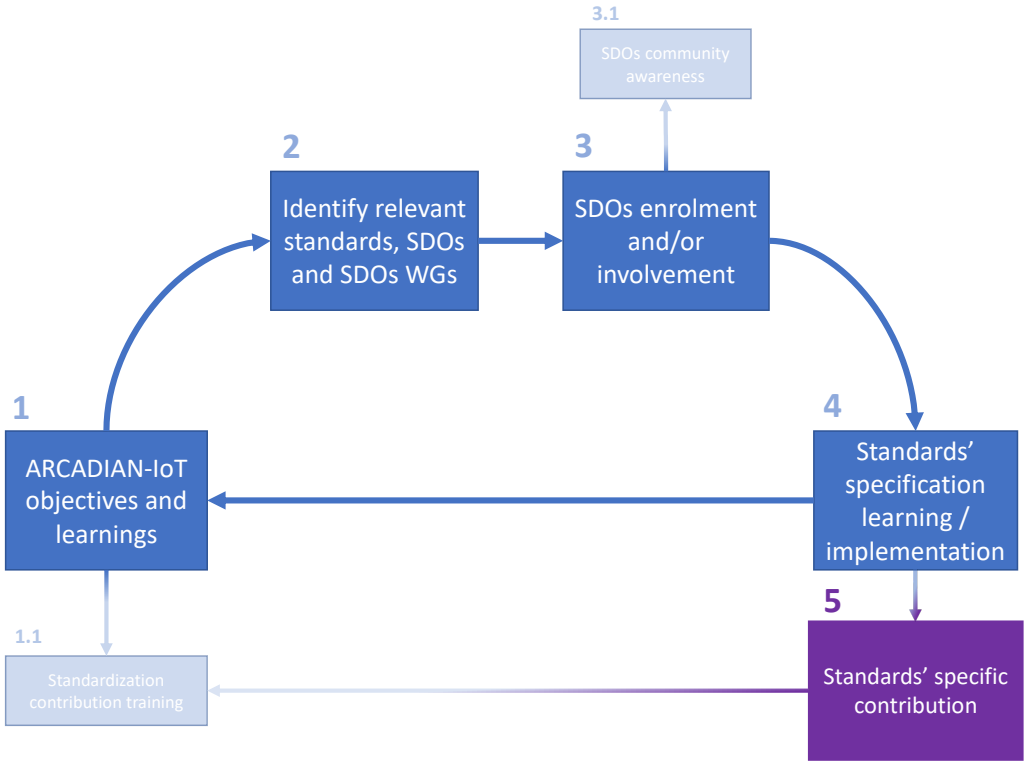

Figure 2 - ARCADIAN-IoT's approach to contribute to standardization

After a first iteration, with the learnings collected throughout the project (1), particularly in the second half, partners were able to select different SDO's Working Groups to monitor or to contribute to (2 and 3), to learn the scope of those standards specifications (4), and to suggest, as specific contributions, potential extensions and new use cases considered relevant according to the project results. This work is part of the standardization roadmap to follow until the end of ARCADIAN-IoT.

3. TARGET STANDARDIZATION BODIES AND INDUSTRY FORA

This section starts by providing a summary of the standardization bodies that relate to the research areas of ARCADIAN-IoT. Then, it focuses on the SDOs and related Working Groups that the partners selected to contribute to, according to their particular research or industrial interests.

3.1. Standardization bodies and industry fora relevant for ARCADIAN-IoT

3.1.1 Overview of ARCADIAN-IoT standardization potential

Given its holistic approach to jointly address Identity, Security, Privacy, Trust, and Recovery capabilities for IoT systems, ARCADIAN-IoT spans a wide range of topics that are relevant from a standardization perspective – either being currently addressed or with untapped potential. In this section, we review the different planes of the framework and associated components, in preparation for the analysis of the relevant Standards Development Organizations (SDOs) in the next sections.

Within the vertical planes (see Figure 1), the **Identity Plane** enables the management of identities of the different entities (e.g., persons, devices and ARCADIAN-IoT components/services), and comprises work on the multiple identification schemes, particularly the Decentralized Identifiers for providing a decentralized digital identity, eSIMs as secure elements capable of storing identity and authentication credentials in the hardware, and Biometrics focusing persons' facial recognition using different devices and considering diverse circumstances (e.g., distance, angle, exposure to light). The **Trust Plane** implements mechanisms for managing the trust policies and levels of the involved entities (persons, devices and services), namely using Verifiable Credentials as a method to enable trusted identification of users and things through the issuing of identity claims; Remote Attestation for attesting IoT device and service integrity with the support of a hardware-based Root of Trust (RoT); Network-based Authorization for enforcing trust-based authorization rules in the network core and informing secure elements about their corresponding device trustworthiness level; and the Reputation System, responsible for determining the different entities' Reputation scores based on data received from other entities and ARCADIAN-IoT components, and defined security policies. Finally, the **Recovery Plane** addresses recovery management of data associated to the different types of entities, concretely the Self-Recovery for enabling heterogeneous devices to access data recovery services according to different access policies, and the Credentials Recovery for secure recovery of credentials, the first and necessary step to trigger data recovery actions.

Within the horizontal planes, the **Privacy Plane** aims to provide functionalities for the privacy-preserving management of confidential or sensitive data both involving persons' and persons, including the (i) Self-aware Data Privacy and (ii) Federated Artificial Intelligence (Federated AI) components. The **Security Plane** contains all the cyber security features required for the monitoring, prevention, management, and recovery. It comprises the (i) Network Flow Monitoring, (ii) IoT Device Behaviour Monitoring, (iii) Cyber Threat Intelligence, (iv) Network Self-protection, (v) IoT Device Self-protection, and (vi) Network Self-healing components. The

Common Plane includes the two components that provide common functionalities to the Vertical Planes, i.e., (i) the Hardened Encryption and (ii) Permissioned Blockchain components.

Some of these areas are addressed by different standardization ecosystems (e.g., Internet-centric, Telco-centric, Cybersecurity), consistently with the fact that ARCADIAN-IoT functionalities may target different segments of the IoT value chain, such as IoT device manufacturers, Mobile Network Operators or MVNOs, IoT service providers or developers, or cybersecurity product vendors.

We performed an updated analysis of relevant standardization areas and associated SDOs, as reported in the next subsections, which is organized according to the most related ARCADIAN-IoT plane.

3.1.2 IoT trust management

The research lines on **Network-based Authorization** (Trust plane) and **eSIM for Network-based authentication** (Identity plane) are both supported by the usage of eSIM. SIM- and eSIM-based communications are areas specified under **GSMA**'s scope. GSMA is one of the main engaged SDOs, for which further detail is presented under section 3.3. The research lines on **Remote Attestation** (Trust plane) of devices leveraging different hardware-based RoT approaches (eSIM or cryptochip) is relevant to multiple identified SDOs. The first one is IETF, in its RATS WG; IETF is also one of the main engaged SDOs, and thus will be presented in more detail in section 3.2. Remote Attestation is also addressed within the Trusted Computing Group (TCG). TCG is aimed at enabling secure computing, such as protection of business-critical data and systems, secure authentication and protection of user identities, or the establishment of machine identity and network integrity. Similarly to other SDOs, its work is organized per WG, e.g., Attestation, Cloud, Cyber Resilient Technologies or DICE. The Remote Attestation work has relevant links to the TCG DICE WG. DICE addresses new approaches for enhancing security and privacy with minimal silicon requirements, where TPMs or similar silicon-based capabilities may or may not be present. The Attestation WG is partially related, with the important constraint being the assumption of the presence of a TPM in the supported systems or components.

3.1.3 IoT identity management

ARCADIAN-IoT is doing research on **Decentralized Identifiers** and **Verifiable Credentials** for supporting IoT devices, services, and person authentication. These technologies are directly linked and are being standardized by the **World Wide Web Consortium (W3C)**[6], an international community where member organizations, a full-time staff, and the public work together to develop web standards (Recommendations). W3C addresses areas such as web design and Applications, Web of devices, Web Architecture, Semantic Web, XML Technology, Web of Services, Browsers

[6] https://www.w3.org/Consortium/

and Authoring Tools, and its work is organized per WG (similarly to the IETF). The most relevant Working Groups include the Verifiable Credentials WG, the Decentralized Identifiers WG and the Device and Sensors WG.

One of the use cases addressed by ARCADIAN-IoT, and where the framework is going to be validated, i.e., the Emergency and Surveillance domain, revolves around the usage of drones for security monitoring of individuals on the move. In such a scope, it has been specified that IoT device identification in ARCADIAN-IoT is supported by DIDs and network credentials. Nevertheless, the IETF DRIP (Drone Identification Protocol) has been identified as potentially relevant and worth monitoring in the future.

3.1.4 IoT privacy

Several proposals in the areas of IoT and privacy, to which **Self-aware Data Privacy** relates, are under standardization within ETSI[7]. ETSI is a European Standards Organization targeting the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services. ETSI standards are organized according to the following technical groups: Technical Committee (TC), ETSI project (allowing participation of members only), ETSI partnership projects, industry specification group, open-source group (allowing participation of both members and non-members).

Within ETSI, TC Cyber is particularly relevant to the scope of ARCADIAN-IoT, as it addresses the areas of protection of personal data and communication or consumer IoT security and privacy,

3.1.5 IoT security

The ARCADIAN-IoT components providing network detection, protection and healing (**Network Self-Protection**, **Network Flow Monitoring**, **Network Self-Healing**), from the Security Plane, are somewhat related to some of the specifications under ETSI TC-CYBER, which additionally addresses network security or cybersecurity tools. Concretely, TC-CYBER considers middleware's an important component for defending network functions, which has led to the creation of Middlebox Security Protocol (MSP). MSP started addressing the usage of MSP for securing Home Gateways and are currently working on Network Routers, optical network and device security. Finally, TC-CYBER has also produced previous work on structured threat information sharing, partially relating to the Cyber-Threat Intelligence work. Another ETSI's TC, SmartM2M[8], addresses standards for enabling M2M services and applications, as well as some aspects of the IoT.

[7] https://www.etsi.org/about

[8] https://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf

Last but not least, the IETF is also producing a significant amount of standardization work specifically supporting IoT cybersecurity, some of which is relevant for ARCADIAN-IoT components to take advantage of or employ (e.g., SUIT, TEEP, CWT, and obviously RATS).

Considering the reasons provided above, the following sections present more details on those organizations and associated WGs where ARCADIAN-IoT has had and is expected to provide more active contribution.

3.1.6 Delimiting scoped SDOs

Given the wide range of areas with standardization potential, it is natural that some of them were prioritized, as a result from a combination of three main factors:

- Relevance of ARCADIAN-IoT results to the standard;
- Partner's individual exploitation goals and strategy;
- Available capacity / skilled resources for engagement in standardization.

Considering the above factors, IETF and GSMA, where ARCADIAN-IoT partners are active, are the focus of the rest of the document. The upcoming sections providing further details on these target SDOs, their relationship to ARCADIAN-IoT and the exact Working Groups in which the consortium has been engaged.

3.2. IETF

3.2.1 Context, mission and objectives

The Internet Engineering Task Force (IETF) is a large, open community of volunteers who collaborate to develop and standardize the protocols and technologies that make up the Internet. It is an international organization that consists of network designers, operators, vendors, researchers, and other interested parties from around the world.

The IETF was established in 1986, and it operates under the auspices of the Internet Society (ISOC). The IETF produces standards mostly through a number of Working Groups, each of which is focused on one specific area of interest, such as Routing, Security, and Transport. The Working Groups are open to anyone who wants to participate, and they collaborate via email, teleconferences, and face-to-face or virtual meetings. Some of the WGs relating or addressing IoT support include CoRE (Constrained RESTful Environments), ACE (Authentication and Authorization for Constrained Environments), CBOR (Concise Binary Object Representation), COSE (CBOR Object Signing and Encryption), LAKE (Lightweight Authenticated Key Exchange), IOTOPS (IoT Operations), TEEP (Trusted Execution Environment Provisioning), RATS (Remote Attestation ProcedureS) or SUIT (Software Updates for the Internet of Things) WG.

The mission of the IETF is to "make the Internet work better" by developing and promoting open standards and best practices. These standards are developed through an open process revolving around building "rough consensus" that involves rigorous technical reviews and open discussions.

The objectives of the IETF are to:

- Develop and promote open Internet standards that facilitate interoperability, security, and innovation, and produce high quality technical documents that describe these standards.
- Provide a platform for the exchange of ideas and technical expertise among network designers, operators, vendors, researchers, and other interested parties.
- Encourage the development and adoption of Internet standards by governments, industry, and other stakeholders.
- Foster the growth and evolution of the Internet by identifying emerging trends and developing solutions to address them.
- Maintain and improve the quality of existing Internet standards by regularly reviewing and updating them.

3.2.2 Related ARCADIAN-IoT work

One of ARCADIAN-IoT partners, RISE, has a long-term and successful track record in IETF standardization of IoT security protocols, especially in the Working Groups CoRE[9], ACE[10], and LAKE[11]. ARCADIAN-IoT is conducting research on cybersecurity components that need to run on IoT devices and communicate with the Internet, e.g., the behaviour monitoring component relying on Federated Learning-based models. In particular, for the Federated AI component, RISE is researching mechanisms for reducing the communication cost during the training phase that requires the interaction among IoT nodes. In this context, attention is being focused on the communication protocols, protection methods applicable to those, and the overhead of those secure communications.

In addition, ARCADIAN-IoT is also researching a new solution for remotely attesting IoT devices and services, benefitting, among other features, from secure elements such as eSIM and cryptochips as hardware-based Roots of Trust and attribute-based encryption (ABE) for enhanced support of multiple Verifiers[12].

Remote Attestation refers to the procedure where evidence about a remote peer is sent and analysed (appraised) for assessing its trustworthiness, being such appraisal performed by either an authorizing entity or with the aid of a third party (Verifier).

[9] https://datatracker.ietf.org/wg/core/about/

[10] https://datatracker.ietf.org/wg/ace/about/

[11] https://datatracker.ietf.org/wg/lake/about/

[12] ARCADIAN-IoT, "D4.2Vertical plane of ARCADIAN-IoT – 2nd version", 2022

3.2.3 Target Working Groups

3.2.3.1 Remote ATteStation (RATS) WG

Previous work from the WG includes the establishment of an architecture (now RFC9334 – Remote Attestation Procedures Architecture) for remotely attesting a peer, i.e., for assessing its level of trustworthiness according to a given policy. The WG intends also to standardize both the formats for describing evidence and attestation results, and the associated procedures and protocols (i.e., for conveying evidence to a verifier and attestation results to a relying party, respectively). Moreover, the WG aims at standardizing formats for endorsements and reference values, potentially applying and/or profiling existing protocols such as DTLS or CoAP to convey them to the verifier.

RATS has synergies and links with other IETF WGs, in some cases in terms of cooperation and coordination. Some examples include:

- TEEP[13]: Remote attestation is needed for running the TEEP protocol, primarily by having a device sending information about its properties / state before operations on trusted applications (installation, update or deletion) are authorized by the Trusted Application Manager. TEE provisioning is also mentioned as an example of remote attestation use case.
- SUIT[14]: In the context of secure firmware updates for IoT, for a bootloader to be considered to have a secure boot, it must produce boost measurements as part of an attestation solution [RFC9019]. The definition of a set of claims for attesting to firmware update status may be produced within SUIT or RATS.
- ACE[15]: this WG has standardized CBOR Web Token (CWT), a compact means of representing and protecting claims to be transferred between two parties. Claims in a CWT are encoded in the Concise Binary Object Representation (CBOR), while CBOR Object Signing and Encryption (COSE) is used for additional application-layer security protection. RATS considers both CWT and JWT as encoding formats to be supported by its information model.

3.2.3.2 Constrained RESTful Environments (CoRE) WG

The Constrained RESTful Environments (CoRE) Working Group focuses on developing standards for Internet of Things (IoT) devices that have limited resources, such as low memory, processing power, and energy. The primary objective of the CoRE Working Group is to enable IoT devices to communicate with each other and with the Internet using RESTful interfaces. To achieve this, the CoRE Working Group has developed several protocols, including CoAP (Constrained

[13] https://datatracker.ietf.org/wg/teep/about/

[14] https://datatracker.ietf.org/wg/suit/about/

[15] https://datatracker.ietf.org/wg/ace/about/

Application Protocol), which is a lightweight and efficient protocol designed for use in IoT devices. CoAP is based on the same architectural principles as the HTTP protocol, which makes it easy to use for developers who are familiar with web technologies. The CoRE Working Group has also developed several extensions to CoAP, including Block-wise transfers, Observing resources, security protocols such as OSCORE for end-to-end message protection, and group CoAP. Overall, the work done by the CoRE Working Group has been critical in enabling the development of IoT devices and applications that can operate efficiently and securely in resource-constrained environments.

CoRE has synergies and links with other IETF WGs, in some cases in terms of related works and cooperation. Some examples include:

- ACE: its primary objective is to enable authentication and authorization of Client devices, when these attempt to access protected resources at Resource Server devices, while offloading the evaluation of access control policies to a trusted third party acting as Authorization Server. The ACE framework relies on a set of building blocks, including OAuth 2.0 and the Constrained Application Protocol (CoAP), where extensions have been introduced to satisfy and better fit IoT devices' requirements.
- LPWAN: this WG aimed to enable IPv6 connectivity using Low-Power Wide-Area (LPWA) technologies: SIGFOX, LoRa, WI-SUN, and NB-IOT. The Working Group is developing new standards to optimize IPv6 communication to end devices and is collaborating with stakeholders to ensure that proposed solutions meet real-world demands. The group has already produced documents on LPWA technologies and a framework for the Static Context Header Compression and Fragmentation (SCHC), which provides both a header compression mechanism and an optional fragmentation mechanism. LPWAN has ceased to exist in March 2023. It has been rechartered in order to address not only LPWAN technologies. The result has in fact the formation of the new Working Group SCHC, where the ongoing work of LPWAN has been migrated.

3.3. GSMA

3.3.1 Context, mission and objectives

GSMA[16] represents the worldwide mobile communications industry. It defines itself as a global organization that unifies "the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change". GSMA's vision is to "unlock the full power of connectivity so that people, industry and society thrive". GSMA members are

[16] https://www.gsma.com/

mobile operators, organisations across the mobile ecosystem and adjacent industries. Its areas of actuation are Industry Services and Solutions, Connectivity for Good and Outreach.

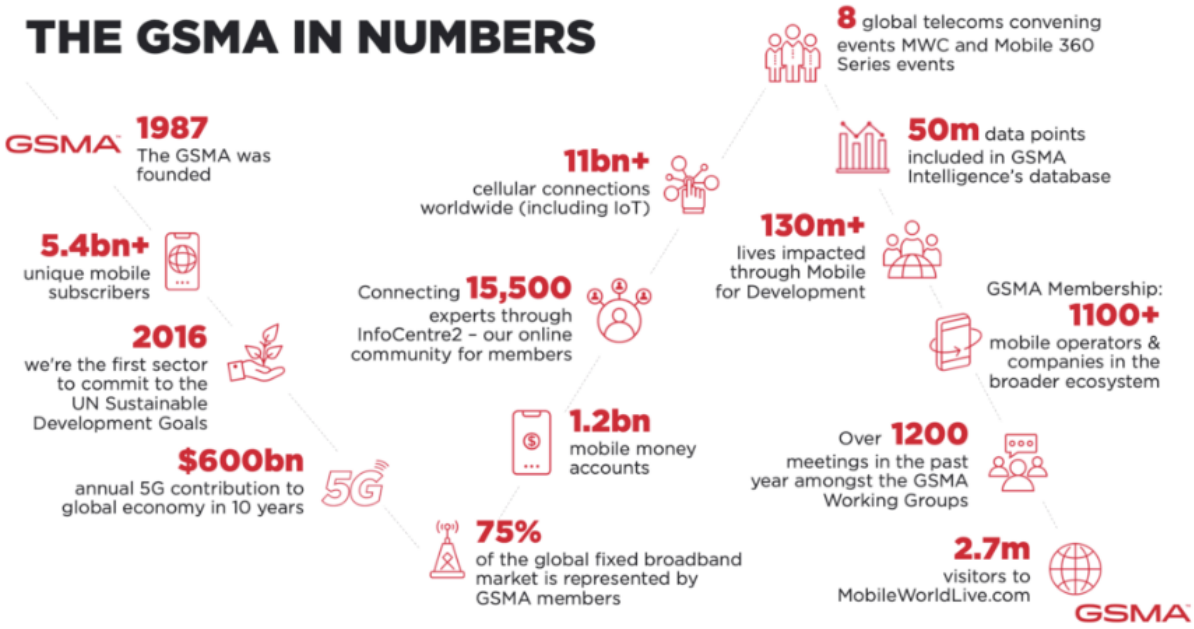

Figure 3- The GSMA in numbers[17]

Regarding the *Industry Services and Solutions*, it is relevant to clarify that GSMA is a global member-led organization that represents the mobile industry. It enables its members to work towards common goals in topics such as 5G, IoT, Roaming, AI, Security and SIM technology, driving discussions, decisions and initiatives that shape the future of mobile communications[17]. Members include MNOs, MVNOs, Satellite Operators, Equipment Providers, M2M Operators, Software Companies, Automotive, Aviation, Manufacturing, and many others[18]. These members form communities per sector (e.g. manufacturing, automotive or aviation) or per technology domain (e.g. IoT and Identity & Data). Other GSMA services in this area are:

- GSMA Foundry, devoted to cross-industry collaboration and business development.
- GSMA Working Groups that focus on the industry priorities and perspectives to engineer the future of connectivity.
- Industry Specifications, facilitated and maintained by GSMA.

[17]https://www.gsma.com/membership/

[18]https://www.gsma.com/membership/membership-types/

In what regards the *Connectivity for Good* area of actuation, GSMA members are unified behind a common industry purpose of Connecting Everyone and Everything to a Better Future [19]. Having the mobile industry as critical for digital transformation and for tackling society's most significant challenges, GSMA members are committed to the UN Sustainable Development Goals, and to perform advances in responsible leadership.

Concerning the GSMA *Outreach* actions, the association organizes some of the most relevant events of the mobile industry, from which excel the Mobile World Congress (MWC), which takes place every year in Barcelona, Las Vegas, Africa (Rwanda in 2023[20]) and Shanghai.

Further details regarding the prominence of GSMA in the mobile industry can be found in Figure 3.

3.3.2 Related ARCADIAN-IoT work

One of ARCADIAN-IoT partners, TRU, is a GSMA member, pioneer in eSIM lifecycle management technologies certified with GSMA's Security Accreditation Scheme (SAS)[21]. In ARCADIAN-IoT, TRU is researching, among other aspects, the use of eSIM as Root of Trust (RoT) for Hardened Encryption, and leveraging network credentials (stored in the Subscriber Identity Module – SIM/eSIM) and authentication mechanisms, to authenticate IoT devices and persons (subscribers) in Cloud services. Considering that eSIM specifications are discussed and managed in GSMA Working Groups, there is a close relation between the work done in ARCADIAN-IoT and GSMA Industry Specifications.

3.3.3 Target Working Groups

Considering the objectives of ARCADIAN-IoT, the most relevant GSMA Working Group is **IoT SAFE**[22]. This Working Group supports that the SIM (any SIM form) is best suited to have a Root of Trust role in an IoT device as it has advanced security and cryptographic features and is a fully standardised secure element, enabling interoperability across different vendors and consistent use by IoT device makers. IoT SAFE relies on the proven SIM to secure IoT data, which is an advantage when compared to using proprietary and potentially less trusted hardware secure elements added to the device. Particularly, IoT SAFE:

- Uses the SIM as a mini "crypto-safe" inside the device to securely establish secure communication with the cloud/server.
- Is compatible with all SIM form factors (SIM, eSIM, iSIM, …).

[19] https://www.gsma.com/betterfuture/

[20] https://www.mwcafrica.com/

[21] https://www.gsma.com/security/security-accreditation-scheme/

[22] https://www.gsma.com/iot/iot-safe/

- Provides a common API for the highly secure SIM to be used as RoT by IoT devices.
- Helps tackling the challenge of provisioning millions of devices.

Despite being a very relevant Working Group that deals with top state of the art IoT challenges, IoT SAFE is still not a mature or well-known standard. In 2022, the Working Group created a marketing sub-group exactly to foster the awareness of the industry regarding this specification.

While IoT SAFE is the most relevant GSMA Working Group for ARCADIAN-IoT, considering the use of eSIM and the focus on cybersecurity, the following Working Groups will also be target of monitoring:

- SIM[23] (general working group) that currently focuses on topics like eUICC[24] Protection Profile; eUICC test specifications; and eUICC specification update and maintenance.
- SAM[25] (Secured Applications for Mobile), which defines a capability allowing cellular connected devices to use a wide range of secured applets within an eUICC.

4. STANDARDIZATION ACTIVITIES AND CONTRIBUTIONS

This section describes the concrete activities of ARCADIAN-IoT partners regarding contributions to standardization processes. The target SDOs /industry fora are the IETF, particularly the RATS, CoRE and SCHC WGs, and GSMA, particularly the IoT SAFE WG (with close monitoring of eSIM and SAM).

4.1. IETF – RATS WG

4.1.1 Participation in relevant WG meetings

ARCADIAN-IoT partners had remote participation in 3 RATS WG sessions, specifically during the meetings IETF 113 (12/3/2022), IETF 114 (25/7/2022) and IETF 115 (7/11/2022).

4.1.2 Mapping of standards in ARCADIAN-IoT work

While the usefulness of Remote Attestation for providing added proof over the integrity of devices (IoT included) is mostly consensual, and being addressed in multiple communities (e.g., IETF, TCG, FIDO, PSA), not every equipment may include (costly) security hardware (e.g., TPMs). ARCADIAN-IoT is thus performing research on remote attestation leveraging alternative HW-

[23]https://www.gsma.com/aboutus/workinggroups/sim-working-group

[24]eUICC is the hardware set in devices to receive eSIM profiles

[25]https://www.gsma.com/newsroom/wp-content/uploads//SAM.01-v1.0.pdf

based Root of Trust approaches, e.g., SIM or cryptochips, and benefiting from Attribute-based Encryption for supporting multiple Verifiers.

The RATS WG focuses on standards for supporting interoperable remote attestation procedures, and addresses items including use cases for remote attestation, augmentations to remote attestation procedures architecture, data models for evidence and attestation results, or usage / extension of existing protocols for the purpose of securely conveying evidence and attestation results, among others. There might be opportunities for proposing alternative approaches remote attestation information / interaction models, based on the work performed in the project, and in the scope of applying the new remote attestation mechanisms in the project's use cases and associated devices / environments (e.g., remote attestation of the drone).

4.1.3 Community awareness actions

The ARCADIAN-IoT work on remote attestation was presented to Fraunhoffer SIT, a major player in the IETF (in RATS and other relevant WGs such as CBOR). This allowed to discuss potential directions for IPN contribution to the IETF RATS WG, for instance relating to the usage of eSIM as a RoT for remote attestation (as an alternative to TPMs or PSA).

4.1.4 Standardization contributions

Up to this point, one active engagement activity has been performed. Concretely, IPN has provided a review of draft-ietf-rats-reference-interaction-models-v06 on the RATS WG mailing list.

4.2. IETF – CoRE and SCHC WG

4.2.1 Participation in relevant WG meetings

One representative of RISE has been chairing the CoRE WG during the last three years, has participated in all its meetings (32 interim online meetings and 6 in-person meetings, counted from May 2021). Also, RISE has been contributing to several Internet Drafts in the CoRE WG. RISE has also started to contribute in the SCHC WG, by means of one Internet Draft and by participating to 2 in-person meetings, during one of which the new proposed Internet Draft has been presented.

4.2.2 Mapping of standards in ARCADIAN-IoT work

ARCADIAN-IoT is researching privacy-preserving Federated AI solutions and their use in the IoT domain. One of the problems is related to the communication cost in federated learning, which requires a large amount of data transmission between the clients and the server during the training process. One approach used in the project to reduce the communication cost consists in deploying communication models and protocols with low overhead. Group CoAP and Group OSCORE,

which are being developed in the CoRE WG, are two protocols suitable for the secure group communication of federated learning with constrained devices.

One possible way to use Group CoAP and Group OSCORE for federated learning is to form a group of devices that share a common machine learning model, and use Group CoAP to exchange updates on their local parameters or gradients. Group OSCORE can provide end-to-end security for the exchanged messages, ensuring confidentiality, integrity, source authentication, and replay protection. By doing so, the devices can collaboratively train the model without compromising their privacy or sending their data to a central server, while attaining a low communication overhead and ensuring end-to-end security.

4.2.3 Standardization contributions

RISE has been regularly participating as key contributor to IETF standardization activities, In particular, Marco Tiloca (RISE) is currently the Chair of the IETF CoRE WG, and a member of the Internet-of-Things Directorate and of the ART Area Review Team.

In the ongoing standardization activities, RISE has co-authored the following documents:

- **Group Communication for the Constrained Application Protocol (CoAP)** in the CoRE WG – a document on the usage of the Constrained Application Protocol for group communication, for example using UDP/IP multicast as the underlying data transport.[26] Group CoAP is adopted as preferred communication means for the IoT devices with Federated AI components, when they need to communicate with one another during the training phase of the ML models.
- **Group OSCORE – Secure Group Communication for CoAP** in the CoRE WG – a document on a method for protecting group communication over CoAP, based on an adaptation of OSCORE.[27] Group OSCORE makes it possible to protect the group communication of IoT devices running the Federated AI component.
- **Clarifications and Updates on using Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)** in the SCHC WG – a document that extends the use of the Static Context Header Compression (SCHC) framework for enabling the compression of CoAP message headers (as defined in RFC 8824).[28] The compression of CoAP message headers helps to reduce the size of the messages exchanged between peers in Federated AI, making the communication more efficient.

[26]https://datatracker.ietf.org/doc/draft-ietf-core-groupcomm-bis/

[27]https://datatracker.ietf.org/doc/draft-ietf-core-oscore-groupcomm/

[28]https://datatracker.ietf.org/doc/draft-tiloca-schc-8824-update/

4.3. GSMA – IoT SAFE

TRU is a pioneer in eSIM technology that has been active in the GSMA for many years (39 active employees in March 2023). Not only it contributes to defining the eSIM specifications and implements them (e.g., eSIM for consumer and IoT), but also participates in GSMA Mobile World Congress with relevant keynotes sharing innovative products and ideas for the Subscriber Identity Modules (SIMs) of the future.

4.3.1 Participation in relevant WG meetings

Considering the close relation between IoT SAFE and the use of eSIM in ARCADIAN-IoT, since the beginning of the project TRU participated in all IoT SAFE WG meetings (8).

4.3.2 Mapping of standards in ARCADIAN-IoT work

In this section, we detail the specific match of IoT SAFE specifications with the project objectives. Overall, the project aims to use the eSIM/eUICC as a trusted hardware capable of assuming the role of Root of Trust (RoT) in IoT cybersecurity mechanisms. This objective is completely aligned with IoT SAFE purpose. However, as previously mentioned, the existing specifications are quite new, with several open change requests and open questions, and their application is still very scarce. Particularly, IoT SAFE application as studied in ARCADIAN-IoT is not found in any state of the art. Considering this, the specification implementation towards the objectives in mind in ARCADIAN-IoT has potential to generate valuable contributions to this GSMA WG. In the next paragraphs are detailed the envisioned uses of IoT SAFE specifications in ARCADIAN-IoT.

Hardened Encryption

One of the roles of eSIM as RoT in ARCADIAN-IoT is to strengthen novel encryption methods. To this end, we propose to use the cryptographic capabilities of the SIM (any SIM form, including eSIM) to generate secrets that allow to digitally sign the encrypted payloads that are communicated to the cloud or stored at the device. These secrets are generated in this hardware secure element of each device and the private part (private key) never leaves it, which is well accepted as secure and highly scalable (the private material is generated at the secure element instead of being provisioned to it and never leaves this safe hardware). The public key is shared externally to be possible to a receiver of the encrypted data to verify the digital signatures and be certain of the data producer identity. The public key will be used as well in use cases of decryption of the data generated in the device by the device itself (after a period of external storage), for the device to be certain that its data is his own / not compromised externally. This process fulfils several relevant cybersecurity properties, like decentralized authentication and non-repudiation, ensuring that attacks like impersonation or data poisoning are easily detected. When mapping this with the IoT SAFE overall architecture (Figure 4), the IoT client application is the encryption method. The IoT Device Middleware is the technology that allows to communicate with the SIM. Finally, the SIM with IoT Security Applet implements the processes described before according to the IoT SAFE specifications.

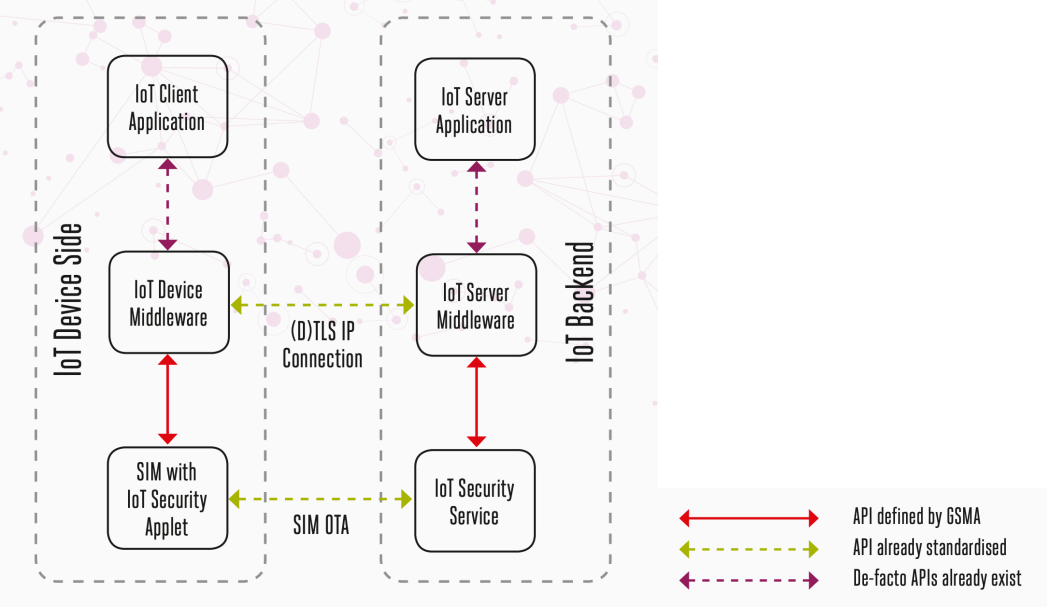

Figure 4 - GSMA IoT SAFE components and overall architecture[29]

Remote Attestation

A similar mechanism is applied in the process of Remote Attestation. In this case, having the secrets already generated and the public keys already distributed, the hardware RoT digital signature increases the robustness of the evidence (set of claims to be appraised by the Verifier) before transmission by the remote device, ensuring its authenticity and non-repudiation properties. The mapping with IoT SAFE is the one described for Hardened Encryption – the Remote Attestation component uses the Hardened Encryption component to get the evidence encrypted and digitally signed by the RoT.

Network-based Authorization and Reputation Information Distribution

A novelty brought by ARCADIAN-IoT is the ability to securely inform the RoT of the trustworthiness of the device where it is installed, allowing it to act accordingly as an independent security agent inside of the device, which may be very relevant in cases where the device is non-cooperative. In the normal operation of the framework, the Reputation System component receives indicators of threats or vulnerabilities from components like Behaviour Monitoring and Cyber Threat Intelligence. This information is normalized in the Reputation System according to trust rules previously defined, e.g., by IoT solution providers and/or CSIRTs, building a trust score for each device. This information is automatically sent to a security component located in the core of the 4G/5G network – the Network-based Authorization. As part of its programmatic operation, this component integrates with eSIM lifecycle management to communicate the trustworthiness information (or trust score), securely and over the air, to the eSIM RoT, which is prepared to

[29]https://www.gsma.com/iot/wp-content/uploads/2020/05/IoT-SAFE-Executive-Summary.pdf

receive and understand it. Looking at Figure 4, in this case the flow is between the IoT Security Service (Network-based Authorization) and the IoT Security Applet, using the standardized SIM OTA communication channel.

Device Self-Protection and Self-Recovery

Having received a trust score of the device where it is installed, the eSIM RoT takes measures of self-protection, if the device is considered compromised, or of self-recovery, in case the RoT receives information that that device used to be compromised and is trustworthy again. Both measures are taken automatically upon reception of the trustworthiness information previously described. The self-protection measure consists of refusing to provide digital signatures to the generated payloads of a compromised device. By not having the expected digital signatures of the data producer in the transmitted payloads, the other ARCADIAN-IoT components and the device owners (e.g., IoT solution providers) can understand that the data in those payloads is not trustable and should be discarded. By discarding this data, several threats may be avoided, like the ones related with poisoned data. This is not the only self-protection measure in the project - it is one more integrated tool available for the framework to ensure security and trust in IoT communications. In the opposite sense, when a device recovers its trustworthiness, the IoT Security Applet resumes its normal operation, as described before. Looking at Figure 4, the process depicted in this paragraph is internal of the IoT Security Applet upon receival of trust related information, and defines the applet behaviour in the interaction with the IoT Device Middleware.

While the baseline for the mentioned processes is IoT SAFE, several extensions to it are being applied. In the next section, we describe the community awareness actions that were considered relevant for the project and for the GSMA IoT SAFE WG.

4.3.3 Community awareness actions

Community awareness actions are considered very relevant to show interest in a particular standard/specification, disseminate the project research objectives and results to a Working Group, but also to disseminate the standards/specifications to communities of interest, to foster awareness and adoption. The GSMA IoT SAFE WG, being recent, strongly feels this need and, in 2022, subdivided its activities in *IoT SAFE technical* and *IoT SAFE marketing* actions, with different meetings for each purpose. In this subsection, we describe community awareness actions taken in ARCADIAN-IoT regarding GSMA IoT SAFE, and regarding the project in that WG.

a. IoT SAFE chair awareness regarding ARCADIAN-IoT

A first awareness action regarding ARCADIAN-IoT to IoT SAFE was held in a meeting with this GSMA WG Chair. In this meeting, the project objectives were introduced, particularly the ones that relate with that community's purpose. The WG Chair also informed about the WG status and next steps. The consortium was invited to provide more awareness regarding the project results when relevant.

b. IoT SAFE WG members awareness regarding ARCADIAN-IoT

The following action, settled with IoT SAFE WG representatives, consisted of informing all the community about ARCADIAN-IoT and its relations with that WG. This happened using the

community mailing list, and triggered follow-up questions from the members. As a result, there was an invitation to present and discuss the ARCADIAN-IoT preliminary results in a plenary meeting.

c. TRU Engineering awareness regarding application of IoT SAFE in ARCADIAN-IoT

There were as well awareness actions regarding ARCADIAN-IoT's work in the IoT SAFE WG to relevant engineering communities. The first one was with TRU's engineering employees in a session led by the company's R&D team. TRU's engineering department is a relevant community because of its expertise and solutions development with eSIM for IoT. Three sessions were held, presenting IoT SAFE and the ARCADIAN-IoT work related with it, two for the general engineering community, with a total attendance of over 130 people, and a third one for executives, key stakeholders for the adoption of the specifications (and of ARCADIAN-IoT) in the industry.

d. Telecommunications industry awareness regarding application of IoT SAFE in ARCADIAN-IoT

Another community awareness action taken was in TAD Summit 2022, an event that joins telecommunication application developers.

Figure 5 - Head of R&D of TRU, presents at TADSummit 2022

This initiative served two general purposes: disseminate ARCADIAN-IoT, particularly the use of eSIM as RoT for cybersecurity, and the use of GSMA IoT SAFE in this project. Considering that the event targeted telecommunications industry stakeholders, and the presence of other SIM/eSIM experts in the audience, creating awareness regarding IoT SAFE specifications was considered relevant.

4.3.4 Standardization contributions

While considering as GSMA IoT SAFE contributions (of *passive engagement*) the enrolment in the WG, the participation in its meetings and the community awareness actions, in this section we highlight *active* or *very active engagement* contributions (see section 2.2 for the considered contribution types). Here we describe, particularly, one where the preliminary results and rationale for the implementation of IoT SAFE specifications in several ARCADIAN-IoT components was presented and discussed in a plenary meeting of that GSMA community, and another related to an open change request to the specifications.

a. Contribution to IoT SAFE plenary meeting with ARCADIAN-IoT preliminary results for analysis

The contribution to the IoT SAFE plenary meeting was triggered by the email sent to this WG mailing list, which raised interest from members in knowing more. ARCADIAN-IoT had a time slot in the meeting agenda with the purpose of not only presenting the project, detailing particularly the use of eSIM as RoT for IoT cybersecurity in several components, but also to discuss the use of the specifications for that purpose and the current implementation results (e.g., performance results can be seen in Figure 6).

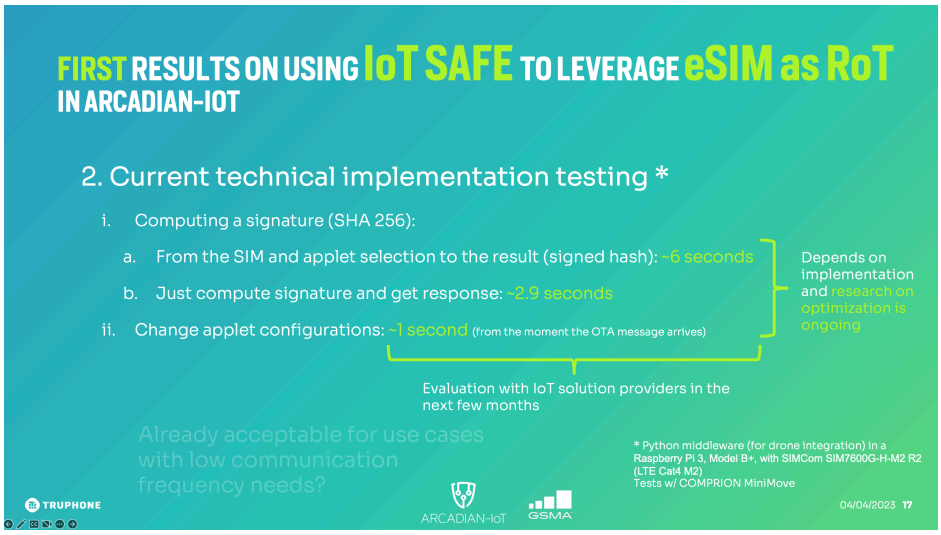

Figure 6 - ARCADIAN-IoT preliminary results in GSMA IoT SAFE plenary meeting

The analysis and the results discussion culminated with a direct request from the WG Chair for TRU to contribute to an open change request: IoT SAFE CR IoT.05 CR002.

Contribution to the change request IoT SAFE CR IoT.05 CR002

The IoT SAFE Chair request to contribute to the *CR IoT.05 CR002* was due to the proven experience implementing the specifications in the context of ARCADIAN-IoT demonstrated in the plenary meeting. The contributions made to this change request consisted of comments with suggestions of solutions to technical open questions. The change request was not closed during the writing of this document.

4.4. GSMA – eSIM and SAM WGs

While the eSIM and SAM WGs are relevant for ARCADIAN-IoT (see section 3.3.2), there is no envisioned active or very active engagement contributions to the industry specifications of these WGs from GSMA. This is because the research hypothesis formulated for using the SIM/eSIM as RoT in ARCADIAN-IoT do not depend on these specifications. Nevertheless, the consortium decided to monitor these WGs by participating to the meetings in order to assess if an opportunity

for contribution arises. However, considering that the eSIM WG has a much higher number of contributors than IoT SAFE and SAM, and considering the need for more activity and awareness for the latter two, GSMA is considering to merge the three Working Groups. This possibility further justifies the continued monitoring of both the eSIM and SAM WGs.

4.4.1 Participation in relevant WG meetings

As previously mentioned, eSIM WGs have more activity than IoT SAFE and SAM. Since the beginning of the project, TRU's R&D team members affected to ARCADIAN-IoT participated in over 36 meetings (plus some without minutes yet) of eSIM and SAM WGs. This accounts to over 50% of eSIM WGs meetings and over 90% of SAM WG meetings.

4.5. Overall summary of current contributions to IETF and GSMA

This section summarizes the contributions from ARCADIAN-IoT to standardization processes in each targeted SDO/industry fora, according to the types defined in section 2.2.

As it can be seen in Figure 7, from the high number of lightweight engagement actions, the participation in standardization meetings of WGs of interest for ARCADIAN-IoT, as well as community awareness actions, became a common practice in the first stage of the project. This is the base that will support the contributions to be made in until the end of the project (April-2024). Nevertheless, 6 actions of active or very active engagement already took place, with ARCADIAN-IoT preliminary results.

	Passive/lightweight engagement[30]	Active engagement[31]	Very active engagement[32]
IETF RATS	4	1	
IETF CoRE	38		2
IETF SCHC[33]	2		1
GSMA IoT SAFE	14	1	1[34]
GSMA eSIM and SAM	36		
Total	**94**	**2**	**4**

Figure 7 - Overall summary of current contributions to IETF and GSMA

5. NEXT ACTIVITIES PLAN

5.1. IETF

Partners plan to continue their contribution to IETF standardization activities in the CoRE, SCHC, and RATS WGs. They will bring their experience matured during the project around group communications for Federated AI in IoT systems, Remote Attestation, and related to ARCADIAN-IoT use cases, to current discussions around open issues for Group CoAP, Group OSCORE, and Remote Attestation. Also, they will continue the writing and updating of active Internet Drafts in the WGs. Overall, the aim will be to contribute to the continued growth and evolution of specifications developed in the CoRE, SCHC, and RATS WGs, as key enablers of cybersecurity for the IoT.

[30] Participation in meetings and community awareness actions

[31] Direct inputs to current documents

[32] Inputs to new documents; implementation of the specifications; results of implementing specifications

[33] The LPWAN WG has ceased to exist in March 2023. The ongoing work of the LPWAN WG has been migrated to the new Working Group SCHC; for this reason, all the activities in the LPWAN WG are practically counted in this document as related to the SCHC WG.

[34]Implementation not provided yet due to the ongoing definition of the exploitation strategy – were provided and discussed the test results in a plenary meeting

5.2. GSMA

As for GSMA the intention is to continue feeding the IoT SAFE community with the results from ARCADIAN-IoT. There are particular needs that were observed in this WG activity that we can address in the course of the project, namely related to the documents *IoT SAFE Common Implementation Guide* and to the *Online Implementation Guide*. Not only can we contribute with our experience related with the implementation of the specifications, but also with ARCADIAN-IoT use cases for using the eSIM as RoT (which is a section in the mentioned documents). The consortium will also consider the need or added value in suggesting any change request to IoT SAFE with the project final outcomes – for example, we will assess the relevance of technical contribution needed to apply IoT SAFE in consumer devices (eSIM as RoT in consumer devices, extending the specifications built for IoT devices). The eSIM and SAM WGs will also continue to be monitored, and contributions will be considered according to ARCADIAN-IoT results and the work from these groups.

6. CONCLUSIONS

Focusing on IoT security, ARCADIAN-IoT has a broad set of standards and industry specifications to consider. While aware of the relevant security standards, the consortium partners decided to target the ones to which ARCADIAN-IoT results could provide relevant contributions, and that are of their interest in terms of exploitation. With this rationale, the IETF, with its Working Groups RATS, CoRE and SCHC, and GSMA IoT SAFE are the SDOs/industry fora and related working groups that ARCADIAN-IoT focuses the most on. The GSMA eSIM and SAM Working Groups are also being actively monitored with the regular participation of the project partners in their meetings.

After the analysis that took the ARCADIAN-IoT consortium partners to the targeted standardization communities, awareness actions were taken, standard specifications were implemented/experimented in the project components, and preliminary results were presented and discussed with SDOs members. Despite not having final results of the project yet, in the course of the initiatives mentioned, several contributions to standardization were already made (see Section 4.3.4).

Leveraging the current involvement and community awareness regarding the project, the focus during the next year will be on using the final results of ARCADIAN-IoT to extend the contributions to the selected standardization bodies.