D8.2

Period 1 Management Report

WP8 – Project Management

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/03/2022
Actual submission date: 31/03/2022

Responsible partner: CNR
Editor: Andrea Saracino;
E-mail address: andrea.saracino@iit.cnr.it

31/03/2022
Version 1.0

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The SIFIS-Home Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-02-2020 GA 952652

Authors: Marko Komssi (FSEC,)Luca Ardito (POL), Andrea Saracino (CNR), Marco Tiloca (RISE), Paolo Mori (CNR) Hakan Lundstrom (SEN), Domenico De Guglielmo (MIND), Tuuli Lindroos (FSEC), Giles Brandon (IC)

Approved by: Giles Brandon (IC)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	20/12/2020	Defined ToC	CNR, IC	All
0.2	13/06/2021	First internal report at M9	IC	1
0.3	01/03/2022	Second Progress Report at M18	IC	All
0.4	15/03/2022	Integrated reviewers comments	CNR	All
1.0	30/03/2022	Definition of User Stories	POL, CNR	All

Executive Summary

This deliverable reports the progress report for the first 18 months of the SIFIS-Home project. The report describes at a high level the activities performed on each work package and task as well as the main achievement of the first half of the project. The project report has followed two iterations: an internal reporting at M9 and a second one at M18.

A more comprehensive report will be delivered together with the financial report for the first review meeting.

Table of contents

1 Explanation of the work carried out by the beneficiaries and Overview of the progress

1.1 *Objectives*

Mission Statements: *SIFIS-Home will provide a multi-level secure, accountable and privacy-aware framework for improving resilience by enforcing and managing application/service security and data protection, as well as for managing in a security-aware manner the smart services typical of a Smart Home environment.*

SIFIS-Home will design, implement and deploy a distributed, resilient, and privacy-aware full-stack architecture that leverages secure communication and management protocols suitable for the IoT, full-lifecycle evaluation and management of software security, machine learning based distributed intrusion detection mechanisms, and privacy preserving data management and analysis techniques. Besides, SIFIS-Home: (i) provides third party developers with APIs, guidelines and automated self-assessment tools to develop certifiable security policy-compliant and privacy-aware applications; and (ii) provides Smart Home users and Smart Home administrators with user friendly interfaces to assess the security and reliability of the services and applications they choose to install, enabling also the definition of simple and easy readable security and management policies, enforced by the framework at all time, ensuring users' safety, security and privacy and improving their trust toward acquisition of new secure interconnected smart home services.

Success criteria: This objective will be achieved through the activities of WPs from 1 to 5 and will be documented by the related deliverables. Full achievement of this objective will be represented by the complete definition and by a demonstration prototype deployed in a realistic environment, of a resilient and efficient architecture for management of security in Smart Home environments, whose resilience to relevant security attacks will be experimentally validated. Another success criterion will be the demonstrated effectiveness of SIFIS-Home in helping developers to design secure applications, whose level of security and compliance to security guidelines will be experimentally verified and certifiable and easy to understand for Smart Home users and administrators.

SIFIS-Home will achieve the following objectives:

Objective 1: *SIFIS-Home will provide an adaptive, intuitive, user friendly and extensible set of secure programming interfaces for developers of Smart Home secure applications and services, which allow the exploitation of the SIFIS-Home framework in its full potential.*
In an interconnected Smart Home environment, applications are the main vectors to introduce vulnerabilities, unwanted or malicious behaviours, representing risks for data privacy, device security and user safety. For this reason, SIFIS-Home will define APIs to write applications by leveraging the namesake framework, which will automatically handle security functionalities and tasks (e.g., the establishment of secure communication associations), thus making them transparent to the developer as much as possible. The novel APIs will leverage and extend the WebThings framework, introducing and improving all security aspects related to secure communication, privacy-aware data management, security event logging, and data encryption.

Success criteria: This objective will be mainly achieved through the deliverables of WP1. An indicator of success is the definition of a well-documented set of APIs (documented in deliverable D1.2) seamlessly integrated in the WebThings libraries, that will integrate in a certified manner the required security functionalities for safe and secure management, communication and data handling provided by the SIFIS-Home architecture described in deliverable D1.4.

Objective 2: *SIFIS-Home will perform research activities on code security and privacy issues by proposing IoT specific metrics and conformance labels for code security and privacy, which will also result in tools for software assessment, aimed at helping developers to write secure and SIFIS-Home compliant application code.*
Software running on IoT devices manages sensitive data, and it should be trusted by users when the context is the Smart Home. In order to be trusted, the code needs to be evaluated against its security level and against how the user (raw) data are managed. This leads to the creation of metrics for evaluating source code, and to provide guidelines and tools for developers for creating secure code by using inherently safer programming languages (e.g. Rust) as well in using static analysis, coverage-guided testing, and sanitization. Developer guidelines will detail the best practices and process to write robust code for smart home applications, and will also focus on how data have to be managed for preserving user privacy. A scoring system based on code security, data management, intrinsic hazard due to use of critical resource and law and regulatory aspects will be created, in order to allow the certification of IoT software artefacts.

Developers, integrators and users will also benefit from a new labelling method, which will perform an evaluation at IoT software level, and IoT infrastructure level based on security and privacy metrics. Labels represented by colours (e.g. red, orange, yellow, green) will assess software running on IoT devices, and infrastructure intended as integration of IoT devices with a focus on the Smart Home scenario.

Success criteria: This objective will be achieved by providing guidelines for developers, a trustworthiness labelling system, and a set of tools to self-evaluate code and application behaviour. Each application will be labelled and will be a tool for users for trusting a software application running on an IoT device deployed in her home. The related activities will be carried out in WP2, and the achievement of the objective will be documented by WP2 deliverables. The guidelines will be tested in the pilot use case activities of WP6.

Objective 3: *SIFIS-Home will provide novel secure communication and management methods and services, as open software components and privacy-friendly building blocks for Smart Home application scenarios.*
The secure communication and management components developed for the SIFIS-Home architecture will build on, exploit, extend, and/or improve cutting-edge security protocols and approaches for the IoT. In particular, they will focus on efficiently and effectively providing highly consistent and trustworthy (inter-network communication among IoT devices, as well as accountable authentication and authorization of IoT devices. This will be achieved through novel solutions and methods that provide: secure (end-to-end) communication and management with support for group communication schemes; management of security credentials, key material, and device lifecycle; enforcement of fine-grained access control policies; and robustness and resilience to denial-of-service attacks.

Success criteria: This objective will be achieved through the deliverables of WP3. Detailed success criteria are: (1) Achieving an effective substantial raise of security and privacy assurances in IoT-based heterogeneous systems for Smart-Home and Smart-Building applications, by building on the elicitation activities of WP1. This will especially focus on secure communication, management of IoT devices and of the networked system as a whole, while ensuring an affordable, limited and controllable impact on performance and user experience. (2) Availability of open, secure solutions and standards for IoT-based networked systems, and especially for Smart-Home and Smart-Building applications. This will fill a major gap currently affecting the IoT security landscape, where several solutions are sub-optimal and proprietary, and most available standardization work is fragmented but yet pioneering.

Objective 4: *SIFIS-Home will adopt a fully privacy-aware approach for data management, and will accordingly design novel privacy-preserving data analysis techniques for smart services that provide transparent security services to identify and tackle misbehaviours and intrusion attempts without hindering users' privacy.*
Data privacy is one of the key elements of the SIFIS-Home project, which aims at ensuring data confidentiality and integrity in all steps of data life-cycle, namely collection, storage, usage and transmission. To this end, the SIFIS-Home project will research, develop or leverage novel mechanisms for data analysis that make it possible to provide services customized to user preferences, without using or disclosing privacy-sensitive information. These mechanisms will be exploited by extending the Deep Speech STT (vocal agent) engine and exploiting generalization and anonymization mechanisms that define user's preferences without linking them to a specific identity. Moreover, a privacy preserving data analysis approach will be used to also provide security services, such as multi-level dynamic intrusion detection and prevention.

Success criteria: This objective will be achieved through the activities of WP4 documented by related deliverables. These deliverables will demonstrate the ability to provide smart services customized according to user's preferences, together with the demonstrated ability of detecting attacks and intrusion attempts in a simulated Smart Home system, without disclosing privacy sensitive information, while proving the adherence to the least-privilege paradigm for the best trade-off between privacy and data utility.

Objective 5: *SIFIS-Home will propose, design, implement, and deploy an architectural model and smart home services designed to ensure verifiable data security at all times.*
SIFIS-Home will be based on a distributed architecture which will allow secure and privacy-preserving communication and management for Smart Home devices. This architecture will also allow the integration of new applications and services in the Smart Home environment, i.e. on top of the smart devices, in a secure and privacy preserving way through the usage of the APIs described in Objective 1. Being distributed, the architecture will also be able to support resiliency.

Success criteria: The achievement of this objective involves the implementation of the SIFIS-Home framework, its deployment on a physical testbed, and its validation on the test cases defined in WP5 against the metrics defined in WP2. The aforementioned implementation will follow the design of the architecture described in deliverable D1.4. The activities to achieve this objective will be performed in WP5, and the results will be described in deliverables D5.3 and D5.4.

Objective 6: *SIFIS-Home will deliver a real-life pilot use case, based on an interconnected Smart Home environment.*
SIFIS-Home will demonstrate both the feasibility and effectiveness of the proposed approach, by deploying the framework in a commercial Smart Home setting provided by MIND and SEN. In particular, a testbed will represent a Smart Home environment, with proof of concept services and applications developed through the SIFIS-Home APIs. The resilience to relevant security attacks will be also demonstrated.

Success criteria: This objective will be achieved through the activities of WP6. In particular, an indicator of success will be the seamless integration of the SIFIS-Home framework in the pilot use case architecture, with a limited impact on performance and with the correct verification of functional applications, the successful fulfilments of security and privacy goals, and the compliance with the security and quality directives provided by the SIFIS-Home project.

Objective 7: *SIFIS-Home will actively disseminate and exploit the project results and will engage in activities devoted to standardize such results.*
SIFIS-Home will effectively and widely advertise and present project results to relevant communities and stakeholders. This will especially leverage publications in academic international venues such as workshops, conferences and journals.

SIFIS-Home will exploit the project results by presenting new commercial opportunities for vendors of security products and for developers of privacy-aware Smart Home applications. This will be achieved by exploiting the influence on the international market of the industrial partners in the consortium, which includes main players in the IT and IoT security market.

SIFIS-Home will actively work on standardizing the project results and developing security solutions in the main international bodies producing open standards for the IT and IoT industry. The project will especially target the premier international standardization body Internet Engineering Task Force (IETF), where RISE and Ericsson have a long-term successful track record in leading IoT security standardization.

Success criteria: This objective will be achieved through the deliverables of WP7. Detailed success criteria are: (1) Publication of scientific papers concerning the project results in the main national and international journals, conferences and workshops, targeting a relevant number of citations. Presentations and distribution of dissemination material (e.g. posters, brochures), advertising the project results at conferences, workshops, exhibitions and other relevant events. (2) Defined exploitation plans from industrial partners on their intended usage of project results to reach a larger set of users and improve business and revenue. (3) Successful standardization process of security solutions developed in the project.

Overview of the project objectives per WP

Objective	Period 1 Achievement
WP1 – Distributed System Architecture *(WP Leader: FSEC)*	
▪ Objective 1.1: Define the architectural model of a resilient, distributed and fault tolerant architecture to manage security and privacy in an interconnected smart home system, while ensuring efficient smart functionalities.	On-Going
▪ Objective 1.2: Elicit architectural functional and non-functional requirements to ensure the functionality of a smart home architecture.	Complete
▪ Objective 1.3: Define privacy and security goals for the SIFIS-Home Security Architecture to effectively improve resilience of smart home systems.	Complete
▪ Objective 1.4: Design prescriptive components for the SIFIS-Home Security Architecture to accommodate functional and security requirements.	On-going
▪ Objective 1.5: Design the whole SIFIS-Home Security Architecture, defining component interaction, interconnections and operative workflow.	On-going
▪ Objective 1.6: Define APIs to interact with the SIFIS-Home Security Architecture, to be made available to developers of SIFIS-Home compliant applications and services.	On-going
WP2 – Guidelines and Procedures for System and Software Security and Legacy Compliance *(WP Leader: POL)*	
▪ Objective 2.1: Define security metrics for evaluating IoT software	On-going
▪ Objective 2.2: Define privacy metrics for evaluating the infrastructure	On-going

▪ Objective 2.3: Deliver proof of concept of tools which evaluate software	On-going
▪ Objective 2.4: Design guidelines that help developers for writing IoT software	On-going
▪ Objective 2.5: Define policy-based software security compliance	On-going
▪ Objective 2.6: Analyse GDPR compliance, licensing compliance and ethical aspects	On-going
▪ Objective 2.7: Trigger and support dissemination, and exploitation of metrics, guidelines and policy in WP7.	On-going
WP3 – Network and System Security *(WP Leader: RISE)*	
▪ Objective 3.1: Design and develop methods and protocols for secure and interoperable communication in the Smart- Home IoT networked infrastructure, with support for group message exchange.	On-going
▪ Objective 3.2: Design and develop methods, solutions and protocols for achieving secure lifecycle management in the Smart-Home IoT networked infrastructure, including access control and key management.	On-going
▪ Objective 3.3: Design and develop methods and protocols for counteracting and reacting against Denial of Service attacks in the Smart-Home IoT networked infrastructure.	On-going
▪ Objective 3.4: Build on the specification and requirements for the distributed system architecture from WP1, and provide feedback for their refinement.	On-going
▪ Objective 3.5: Trigger and support the integration and testing of the developed security solutions within the proof-of- concept implementations undergoing testing in WP5.	On-going
▪ Objective 3.6: Trigger and support the integration of the developed security solutions within the smart home use case undergoing demonstration in WP6.	On-going
▪ Objective 3.7: Trigger and support dissemination, standardization and exploitation of developed solutions in WP7.	Ongoing
WP4 – Privacy-Aware Analytics for Security and Services *(WP Leader: CNR)*	
▪ Objective 4.1: Design and develop novel approaches for identifying unwanted system, device, and application behaviour through multi-domain features extracted by different levels of the smart home architecture software stack, namely from kernel to user level.	On-going
▪ Objective 4.2: Propose innovative mechanisms based on AI and deep packet inspection for preventing network- based attacks such as QoS, DoS, side-channel attacks, hijacking, phishing, replay attacks.	On-going
▪ Objective 4.3: Design, adapt, and customize privacy preserving analysis techniques to provide smart and advanced services to users, while ensuring the privacy of the inferred information and of the user preferences.	On-going
▪ Objective 4.4: Research innovative techniques for detecting statically and dynamically possible misbehaviours of applications, by analysing their executable and/or the list of used APIs.	On-going
▪ Objective 4.5: To perform dedicated research activities for voice analysis and speech recognition to ensure an efficient and effective service, comparable with available commercial solutions, while ensuring data privacy, and avoiding user's profiling.	On-going
WP5 – Integration, Testing and Demonstration *(WP Leader: SEN)*	
▪ Objective 5.1: Implement the architecture designed in WP1, by integrating the solutions developed in WP3 and WP4 and by deploying them in a fully featured testbed.	On-going
▪ Objective 5.2: Define, design and deploy a fully featured physical testbed to deploy the SIFIS-Home architecture and to test and validate the implemented functionalities using state of the art deployment and integration tools.	On-going
▪ Objective 5.3: Implement the user interface components of SIFIS-Home, in particular the Configuration Portal and the Application Marketplace by leveraging tools and technologies provided by SEN.	On-going

▪ Objective 5.4: Define which methods, protocols and tools should be implemented and tested with the complete IoT system in the testbed, to secure a full test coverage of developed components in the project.	On-going
▪ Objective 5.5: Define test cases to validate each developed security component supporting the defined metrics in WP2 and the acceptance tests defined in WP1.	On-going
WP6 – Smart Home Use Case *(WP Leader: MIND)*	
▪ Objective 6.1: Deploy the SIFIS-Home framework in the Mind architecture to implement the use case.	On-going
▪ Objective 6.2: Apply the quality handbook guidelines and exploit the development tools to implement or improve the quality of real commercial application and services for smart home systems.	On-going
▪ Objective 6.3: Integrate the SIFIS-Home marketplace and configuration interface in the Mind platform for integration of third-party services and improved user management.	On-going
WP7 - Dissemination, Standardization and Exploitation *(WP leader: FSEC)*	
▪ Objective 7.1: Develop and maintain the project website, as well as material for project presentations.	Complete
▪ Objective 7.2: Organize training sessions and workshops related to the project's activities.	On-going
▪ Objective 7.3: Ensure an effective dissemination of project results, especially through publications in national and international venues, as well as demonstration platforms and pilots.	On-going
▪ Objective 7.4: Ensure an effective contribution to standardization activities in international bodies.	On-going
▪ Objective 7.5: Ensure an effective planning for commercial exploitation of solutions developed in the project.	On-going
WP8 – Project Management *(WP Leader: IC)*	
▪ Objective 8.1: Collate Deliverables, Milestones and Reports	On-going
▪ Objective 8.2: Manage Legal, Contractual, Financial, Ethical and Administrative Matters	On-going
▪ Objective 8.3: Ensure Communication between Partners	On-going
▪ Objective 8.4: Manage Scientific and Technical Activities	On-going
▪ Objective 8.5: Organise Project Steering Committee	On-going

1.2 *Explanation of the work carried per WP*

1.2.1 WP1: Distributed System Architecture

Objectives (Copied from Annex I - Description of Action)

- Objective 1.1: Define the architectural model of a resilient, distributed and fault tolerant architecture to manage security and privacy in an interconnected smart home system, while ensuring efficient smart functionalities;
- Objective 1.2: Elicit architectural functional and non-functional requirements to ensure the functionality of a smart home architecture;
- Objective 1.3: Define privacy and security goals for the SIFIS-Home Security Architecture to effectively improve resilience of smart home systems;
- Objective 1.4: Design prescriptive components for the SIFIS-Home Security Architecture to accommodate functional and security requirements;
- Objective 1.5: Design the whole SIFIS-Home Security Architecture, defining component interaction, interconnections and operative workflow;
- Objective 1.6: Define APIs to interact with the SIFIS-Home Security Architecture, to be made available to developers of SIFIS-Home compliant applications and services.

Progress per Task

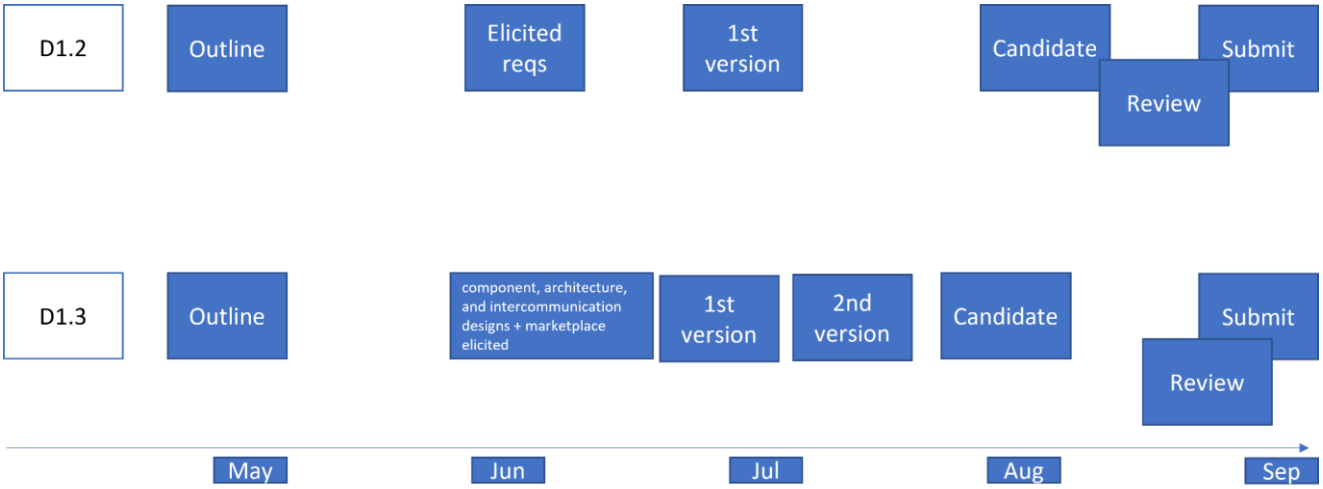
Task T1.1: System Requirements Elicitation (M1-M12/FSEC)

The task started at the beginning of the project according to plan. The main role of T1.1 is to elicit and determine the requirements for the SIFIS-Home Security Architecture. We started the periodic and hands-on meetings in the beginning of the project to manage the elicitation of the requirements from both the end-user and technical points of view. The requirements were elicited according to the use cases of partners, from standards, and based on the partners' existing customer and technical knowledge.

T1.1 activities resulted in the first deliverable of WP1, D1.1 "Initial Architecture Requirements Report" that was submitted on schedule in March 2021. WP1 defined a research methodology to formalize the work. In the deliverable, the initial requirements with priorities were introduced. The requirements were categorized in seven categories as follows:

- 46 functional requirements
- 27 performance requirements
- 2 reliability requirements
- 2 availability requirements
- 20 usability requirements
- 19 dependability requirements
- 29 security requirements

After the D1.1 release, T1.1 started the preparation of D1.2 and supporting the preparation of D1.3. Both D1.2 and D1.3 had a deadline in M12. We managed the authoring of multiple deliveries at the same time with a specific plan that is illustrated in the figure below.



The deliverables D1.2 and D1.3 have been delivered on time at M12, closing the activities of this task.

Task T1.2: Security and Privacy Goals (M3-M12/ CNR)

In the first 6 months of activity this task has defined a list of security relevant architectural requirements on the aspects of privacy, security, access control, integrity of data and devices. The requirements have been extracted partially as functional requirements and partially as non-functional requirements, by following the requirement elicitation methodology already used in T1.1.

The task has been completed at M12 with the release of the deliverable D1.2 where the complete list of security related requirements has been reported, after integrating the feedbacks received from WP3 and WP4 from respectively D3.1 and D4.1.

The activities of this task have involved CNR as leader of the activity, POL and FSEC as main contributors. The results of this task have been included in D1.1 and are being used for D1.2, which will complete the objectives 1.1 and 1.3.

Task T1.3: Definition of Secure Component Design, System Architecture, and Intercommunication (M6-M24/ FSEC)

The task started in M6 according to plan. While T1.1 focuses on requirements, T1.3 focuses on the design of the SIFIS-Home Security Architecture, defining components, functionalities, interconnections and operative workflows. This task has been contributing to D1.3 which has a deadline in M12.

The architecture design has been carried out during “hands-on” telco calls. Unfortunately, face-to-face meetings have not been possible between the partners. To overcome the challenge, the partners have used collaborative methods to design the architecture. We chose to use a tool called Miro (https://miro.com/) to carry out collaborative design in real-time. The figure below illustrates an example of our preliminary design on the high-level components in Miro. Accordingly, D1.3 has been submitted on time at M12.

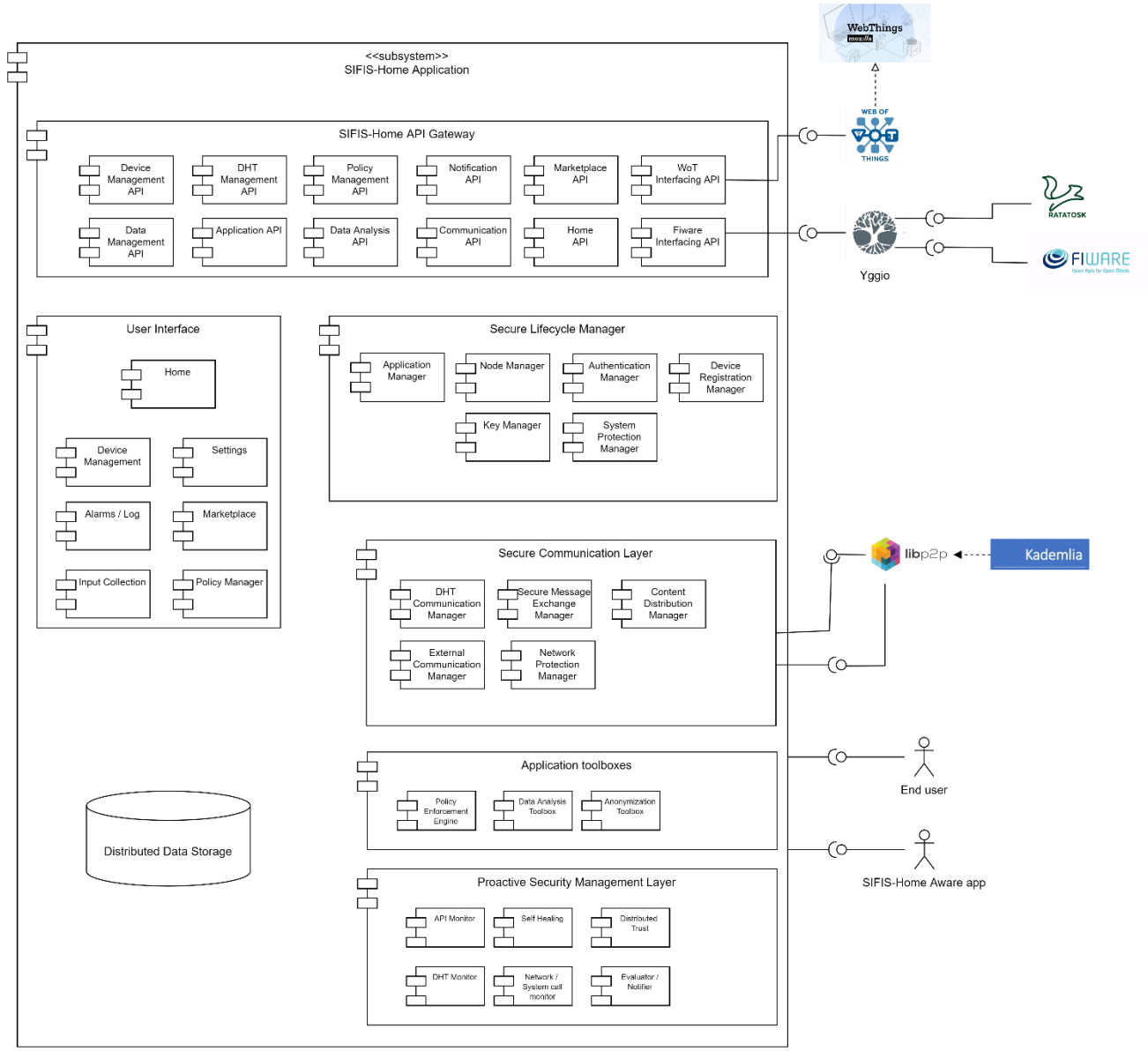


Figure 1: The SIFIS-Home framework as presented in D1.3

In the last 6 months this task has worked in strong cooperation with WP5, by organizing joint WP1-WP5 meetings to work on the final version of the SIFIS-Home architecture and the operational workflows to be included in D1.4. The deliverable is progressing as expected.

Task T1.4: Definition of Secure Development APIs (M6-M24/ POL)

T1.4 started in M6 as planned. It aims at defining a set of APIs for the development of SIFIS-Home compliant applications and services.

This task is tied with T1.3 because it defines how the components defined in T1.3 are connected together, and how they can be invoked.

During M6-M12 there have been preliminary evaluations of the architecture proposed in T1.3 and a preliminary version of the APIs has been introduced in D1.3, released in M12. In the last 6 months this task has been dedicated to defining the API semantic and all the APIs relatable to the workflows of task T1.3.

Achievements

During the reporting period, the following have been achieved:

- The first deliverable of WP1, D1.1 "Initial Architecture Requirements Report", was submitted on schedule in March 2021.
- All use cases and requirements for the SIFIS-Home framework and architecture have been defined and reported in deliverable D1.2.
- WP1 has been a main contributor to milestones MS1, MS2 and MS3.
- The first version of the SIFIS-Home architecture and SIFIS-Home framework have been released and published in D1.3.
- The second set of deliverables has been delivered on time at M12.
- The format of APIs has been defined, together with a preliminary set of APIs partially presented in D1.3 and that will be finalized in D1.4.
- All the WP1 partners have actively participated in the periodic and hands-on meetings of WP1 and WP5.

1.2.2 WP2: Guidelines and Procedures for System and Software Security and Legacy Compliance

Objectives (Copied from Annex I - Description of Action)

- Objective 2.1: Define security metrics for evaluating IoT software;
- Objective 2.2: Define privacy metrics for evaluating the infrastructure;
- Objective 2.3: Deliver proof of concept of tools which evaluate software;
- Objective 2.4: Design guidelines that help developers for writing IoT software;
- Objective 2.5: Define policy-based software security compliance;
- Objective 2.6: Analyse GDPR compliance, licensing compliance and ethical aspects;
- Objective 2.7: Trigger and support dissemination, and exploitation of metrics, guidelines and policy in WP7.

Progress per Task

Task T2.1: Guidelines for IoT Software Development and definition of Security and Privacy Metrics (M1-M24/POL)

The task started in M1 as planned, and targeted designing developers' guidelines for writing secure, privacy-aware, and policy-based IoT software, and developing toolchains and software analyzers, which provide quality metrics of a given source code.

During M9-M18 the main partners have engaged in several, regular technical discussions. The WP2 partners have actively participated in the periodic and hands-on meetings of WP1 and WP5, and WP6. The role of WP2 participants in other WPs is to investigate the toolchain used to develop the software and provide support for the required build system and programming languages to the software tools designed in T2.2 for Quality/Security Evaluation. Furthermore, WP5 and WP6 will soon provide feedback to the Guidelines for IoT Software Development.

Activities during M9-M18 POL and LUM have focused on writing developers' guidelines for producing secure and privacy-aware software, and in developing a tool to ease creating new projects and/or updating pre-existing projects with a base CI setup. Furthermore, the research activities involved the design of a software tool, which provides quality metrics to a given source code. The implementation activity involves T2.2.

The results achieved by this task are reported in D2.1 and D2.2

Task T2.2: Dynamic Code Quality/Security Evaluation (M12-M30/ LUM)

Task started in M12.
A tool to ease creating new projects and/or updating pre-existing projects with a base CI setup had been developed. The partners are slowly setting up their code in the public Github while extended tools to evaluate the code coverage weighted by the underlying code complexity are being finalised. Once the all the code in use for the WP5 and WP6 tasks is deployed it will be evaluated and the partners will receive suggestions and feedback to be addressed in the following months.

The results achieved by this task will be reported in D2.3 planned for release in M24.

Task T2.3: Policy-based Software Security Compliance (M12-M30/ CNR)
Task due to start in M12. During the last six months, this task has been dedicated at defining the building blocks of security policies, building upon the results of T2.1 and T2.2. In particular CNR and POL are working at the definition of policies with conditions related to security, privacy and safety of the SIFIS-Home architecture. The activities are being conducted in cooperation with WP4, which is providing the technological tools for policy writing and evaluation.
The results of this activity will be reported in D2.5.

Task T2.4: Legal Aspects and GDPR Compliance (M1-M30/ POL)
The task started in M1 as planned, and targeted designing mechanisms and formalisms for defining, specifying and verifying behavioural policies for secure applications. The project activities were analysed and areas of intervention identified to make the obligations imposed by privacy regulations an opportunity for the project.

In particular, work was carried out to identify the obligations that must be fulfilled by the different actors involved in SIFIS-Home technologies and labels to make it easier for those using SIFIS-Home technologies to comply with privacy obligations.
During the period M9-M18 the following activities were performed:

- refinement of the list of obligations provided by GDPR and other privacy EU rules to be fulfilled by the different actors involved in SIFIS-Home technologies;
- identification of tools for compliance with GDPR obligations;
- analysis relating to compliance with the obligations imposed by free software / open source licences on software reused;
- identification of tools for compliance with obligations provided by free software / open source licenses;
- ethical analysis of SIFIS-Home technologies with the goal to maximise user control;
- drafting of action points to design some dashboards that reuse tools already available and add further tools to SIFIS-Home technologies.

The results of these activities where documented in D2.6 (Initial Report on Legal and Ethical Aspects) released in March 2022..

Achievements

During the reporting period, the following have been achieved:

- The second deliverable, namely D2.2 “Preliminary Developer guidelines”, has been completed, and submitted on schedule in September 2021.
- The third deliverable, namely D2.6 “Initial Report on Legal and Ethical Aspects”, has been completed, and submitted on schedule in March 2022.
- D2.3 “First Version of Developer tools” is in progress, and it will provide Code and Documentation of the developer tools created in the project that implement some of developer guidelines for assessing IoT software It will be released in M24.
- Discussions with WP1, WP4, WP5, and WP6 have been engaged regarding legal aspects.

1.2.3 WP3: Network and System Security

Objectives (Copied from Annex I - Description of Action)

- Objective 3.1: Design and develop methods and protocols for secure and interoperable communication in the Smart- Home IoT networked infrastructure, with support for group message exchange;
- Objective 3.2: Design and develop methods, solutions and protocols for achieving secure lifecycle management in the Smart-Home IoT networked infrastructure, including access control and key management;
- Objective 3.3: Design and develop methods and protocols for counteracting and reacting against Denial of Service attacks in the Smart-Home IoT networked infrastructure;
- Objective 3.4: Build on the specification and requirements for the distributed system architecture from WP1, and provide feedback for their refinement;
- Objective 3.5: Trigger and support the integration and testing of the developed security solutions within the proof-of- concept implementations undergoing testing in WP5;
- Objective 3.6: Trigger and support the integration of the developed security solutions within the smart home use case undergoing demonstration in WP6;
- Objective 3.7: Trigger and support dissemination, standardization and exploitation of developed solutions in WP7.

Progress per Task

Task T3.1: Secure, Interoperable and Robust Communication (M3-M33/ RISE)
The task started in M3 according to plan. Its targeted security solutions under current design and development focus on securing device operations, interactions and communication. Main topics include secure end-to-end network message protection with support for group communication, as well as counteraction against Denial of Service attacks. The work on these topics largely takes as main building blocks two standard protocols for the IoT, namely the web-transfer protocol CoAP and the secure communication protocol OSCORE.

The main design partners have engaged in several, regular technical discussions and are effectively progressing the design and development activities according to plans. Task T3.1 is tightly related to T3.2, as the respectively developed security solutions are closely related and serving each other. However, the relation between the two tasks and the execution of their interrelated activities have been smooth and natural.

Task T3.2: Security Lifecycle Management (M3-M33/ RISE)
The task started in M3 according to plan. Its targeted security solutions under current design and development focus on administrative/management security services, spanning over the network and device lifecycle. Main topics include authorization, access and usage control of resources and services, as well as establishment, management and renewal of security (keying) material.

The main design partners have engaged in several, regular technical discussions. Task T3.2 is tightly related to T3.1, as the respectively developed security solutions are closely related and serving each other. However, the relation between the two tasks and the execution of their interrelated activities have been smooth and natural.

Task T3.3: Dynamic Multi-Domain Security and Safety Policy Handling (M3-M33/ CNR)
The task started in M3 according to plan and has carried out two activities. On one hand, the task has provided feedback and contributions on the definition of specific access control and usage control

requirements and goals, as related to the evaluation of application and network communication security policies. On the other hand, the task has focused on effectively combining the enforcement of access control and usage control, by building on solutions developed in Task T3.2 and enhancing them with advanced, dynamic policy evaluation.

For both activities, the main design partners have engaged in several, regular technical discussions.

Overall, during M3-M18, activities in all the three tasks above have focused on: i) carrying out the design and specification of the pertaining security solutions mentioned above; as well as on ii) providing analysis and feedback on architecture requirements and goals to WP1, based on the ongoing development of such solutions.

The former point contributed to fulfil the related Milestone MS2 “First architecture and component design” (September 2021), by providing contributions to the definition of the SIFIS-Home architecture specified in deliverable D1.3 “First architecture and component design” (September 2021).

The latter point contributed to fulfil the related Milestone MS1 "Initial requirement elicitation" (March 2021), by providing contributions to the definitions of the SIFIS-Home architecture requirements and goals, and resulted in the released deliverable D3.1 "Analysis and feedback on architecture requirements and goals" (May 2021). In particular, deliverable D3.1 considered what was specified in deliverable D1.1 “Initial Architecture Requirement Report” (March 2021) and provided feedback on and proposal for extending and refining the original set of requirements and goals documented thereof. Such feedback and proposed amendments were adopted in deliverable D1.2 “Final Architecture Requirement Report” (September 2021), hence also contributing to fulfil the related Milestone MS3 “Requirement refinement” (September 2021).

Finally, WP3 has released deliverable D3.2 "Preliminary report on Network and System Security Solutions" (March 2022), which describes the security solutions developed within WP3 at present. In particular, each of those has been explicitly put in relation to the pertaining requirements defined in deliverable D1.2 as well as to the pertaining SIFIS-Home architecture components defined in deliverable D1.3.

Achievements

During the reporting period, the following have been achieved:

- The first deliverable of WP3, namely D3.1 “Analysis and feedback on architecture requirements and goals”, was submitted on schedule in May 2021. The deliverable also provides a brief, high-level overview of the technical security solutions under development in WP3.
- The second deliverable of WP3, namely D3.2 “Preliminary report on Network and System Security Solutions”, was submitted on schedule in March 2022. Each of the presented security solutions has been explicitly put in relation to the pertaining requirements defined in deliverable D1.2 as well as to the pertaining SIFIS-Home architecture components defined in deliverable D1.3.
- Beyond what is documented in deliverable D3.1, WP3 has provided a broader set of feedback and input about deliverable D1.1 to WP1. These have been considered to produce a consolidated collection of requirements and goals documented in deliverable D1.2.
- Progress has been regular and considerable in the design and development of the security solutions in the scope of WP3. Also, the ongoing work has been duly taken as input to related

standardization activities documented in deliverable D7.2 “Preliminary Standardization Report” (March 2022).

1.2.4 WP4: Privacy-Aware Analytics for Security and Services

Objectives (Copied from Annex I - Description of Action)

- Objective 4.1: Design and develop novel approaches for identifying unwanted system, device, and application behaviour through multi-domain features extracted by different levels of the smart home architecture software stack, namely from kernel to user level;
- Objective 4.2: Propose innovative mechanisms based on AI and deep packet inspection for preventing network- based attacks such as QoS, DoS, side-channel attacks, hijacking, phishing, replay attacks;
- Objective 4.3: Design, adapt, and customize privacy preserving analysis techniques to provide smart and advanced services to users, while ensuring the privacy of the inferred information and of the user preferences;
- Objective 4.4: Research innovative techniques for detecting statically and dynamically possible misbehaviours of applications, by analysing their executable and/or the list of used APIs;
- Objective 4.5: To perform dedicated research activities for voice analysis and speech recognition to ensure an efficient and effective service, comparable with available commercial solutions, while ensuring data privacy, and avoiding user's profiling.

Progress per Task

Task T4.1: Multi-level Anomaly and Misbehaviour Detection and Prevention (M3-M33/CNR)

The task has been led by CNR and RIO has been a main contributor. The work has been carried out as planned. Three analytics have been designed and developed within this Task, starting from the study we made in deliverable D4.1 "Analyses and Feedback on Architecture Requirements and Goals" and consistently with the requirements presented in the deliverable D1.2 "Final Architecture Requirements Report", in order to be applicable to the use cases and IoT-based Smart Home environment taken into account in the SIFIS-Home project. The analytics developed within this task are called: Device Fault Detection (CNR), Device Activity Monitoring in Centralized Cloud (RIO), and Parental Control (CNR). For each of these analytics a reference implementation has been developed and some preliminary tests have been executed. These activities are relevant to the Objectives 4.1 and 4.4.

Task T4.2: Network Intrusion Detection (M3-M33/CEN)

FSEC, RIOTS and CEN have been participating in this task. Work has started as planned. Task meetings have been called every other week than WP meetings. During these meetings everyone has present their ideas, possible approach as well as goal support capabilities. Task partners have provided input for respective sections of deliverable D4.1, which was submitted on schedule in May 2021.

Within T4.2 only network flow data will be processed. Possible input data on network-based intrusion detection has been listed as follows: packet timestamp, packet length, source IP address and port, destination IP address and port. It is also possible to see into the packet, if the message is not encrypted. This data will be studied using artificial intelligence functions. The functions to be used have not been finalised yet, but different possibilities have been studied. Promising technologies include NetSpot, Autoencoders and Tensorflow/Keras. Also, other analysis methods may eventually be used.

Task T4.3: Analytics for policy enforcement (M3-M33/ POL)

The task has been lead bu POL, and proceeded as planned. Stemming from the requirements defined at M9, the first months (M9-M12) have been dedicated to the definition of the architecture of the Policy Enforcement Point (PTP), i.e., the module that is responsible to translate and check high-level privacy policies such as "Do not record sound in the living room tonight". In parallel, an OWL ontology named

sifis-home ontology has been created to support the translation procedure and the detection of possible run-time problems like inconsistencies and redundancies between high-level security policies. The remaining months (M13-M18) have been mainly dedicated to preliminary implementation of the PTP module, composed of a Java-based web-server and a web-based user interface. In the last two months (M17-M18), in particular, the implementation was assessed through a set of sample high-level policies, and a video of a demo was designed and created to demonstrate the capabilities of the PTP module.

To summarize, the work carried out during the reporting period has enabled:

- the definition of the architecture of the PTP module;
- the design and implementation of the Sifis-Home ontology;
- the preliminary implementation of the PTP web-server;
- the preliminary implementation of a web-based user interface for defining, checking, and translating high-level security policies;
- a preliminary assessment of the PTP module through the definition, checking, and translation of a set of sample high-level security policies;
- the design and creation of a demo video.

Task T4.4: Privacy Aware Speech Recognition and Smart Service Analytics (M3-M33/ CNR)

The task has been led by CNR, and the work has been carried out as planned. One analytics has been designed and developed within this Task, called Privacy Aware Speech Recognition, still in accordance with study presented in deliverable D4.1 “Analyses and Feedback on Architecture Requirements and Goals” and consistently with the requirements presented in the deliverable D1.2 "Final Architecture Requirements Report". A preliminary reference implementation has been developed and some preliminary tests have been executed. Moreover, CNR also studied a set of techniques for preserving privacy of sensitive data that will be exploited to perform privacy preserving data analysis with the previously mentioned analytics. These activities are relevant to the Objectives 4.3 and 4.5.

Achievements

During the reporting period, the following have been achieved:

- Provided feedbacks to the SIFIS-Home framework and architecture design through deliverable D4.1 submitted at M8.

- The second deliverable of WP4, namely D4.2 "Initial Design and Development of Privacy Aware Analytics for Secure Services", was submitted on schedule in March 2022.
- Performed research activity relevant for more than 4 scientific papers published in top level journal and conferences.
- Developed relevant analytics for the SIFIS-Home framework.
- Provided the end point for inclusion of the analytics in the Analytics Toolbox component of the SIFIS-Home framework

1.2.5 WP5: Integration, Testing and Demonstration

Objectives (Copied from Annex I - Description of Action)

- Objective 5.1: Implement the architecture designed in WP1, by integrating the solutions developed in WP3 and WP4 and by deploying them in a fully featured testbed;
- Objective 5.2: Define, design and deploy a fully featured physical testbed to deploy the SIFIS-Home architecture and to test and validate the implemented functionalities using state of the art deployment and integration tools;
- Objective 5.3: Implement the user interface components of SIFIS-Home, in particular the Configuration Portal and the Application Marketplace by leveraging tools and technologies provided by SEN;
- Objective 5.4: Define which methods, protocols and tools should be implemented and tested with the complete IoT system in the testbed, to secure a full test coverage of developed components in the project;
- Objective 5.5: Define test cases to validate each developed security component supporting the defined metrics in WP2 and the acceptance tests defined in WP1.

Progress per Task

Task T5.1: Testbed Design (M12-M30/INT)
This task started in M12. In the last 6 months of activities the partner of WP5 lead by SEN, have deployed a development and code deployment environment on a server hosted by CNR. Moreover, three testbeds have been defined and the first testbed has been deployed using Docker. The description of the testbed will be reported in the upcoming deliverable D5.1.

Task T5.2: Component Implementation, Integration and Deployment (M12-M33/ SEN)
This task started in M12. In the last 6 months this task has been extremely active starting its cooperation with T1.3 and T1.4 for the implementation of the SIFIS-Home architecture and SIFIS-Home framework. The task is providing feedbacks to T1.3 and T1.4 for finalizing also the SIFIS-Home framework design, identifying possible missing components. All partners are involved in this activity. The task is also done in cooperation with WP6, and in the last month technical meetings involving partners from WP1, WP5 and WP6 have been conducted with a twice per-week schedule.

Task T5.3: Evaluation and Validation (M20-M33/ LUM)
Task due to start in M20.

Achievements

During the reporting period, the following results have been achieved:

- A development and deployment framework has been deployed and made available to all SIFIS-Home partners to integrate the technical solutions coming from the technical WPs.
- Three testbeds have been defined, an emulated testbed, a simulated one and a physical one. The emulated testbed has already been deployed on a server hosted by CNR.

1.2.6 WP6: Smart Home Use Case

Objectives (Copied from Annex I - Description of Action)

- Objective 6.1: Deploy the SIFIS-Home framework in the Mind architecture to implement the use case;
- Objective 6.2: Apply the quality handbook guidelines and exploit the development tools to implement or improve the quality of real commercial application and services for smart home systems;
- Objective 6.3: Integrate the SIFIS-Home marketplace and configuration interface in the Mind platform for integration of third-party services and improved user management.

Progress per Task

Task T6.1: Use Case Requirements Elicitation (M15-M20/MIND)
The activities of this task started with a series of meetings during which MIND explained in detail the various functionalities and characteristics of its devices and platform. Then, the other partners contributed by providing the list and the details of the devices that they are going to use for WP6 demonstrations. Also, a number of possible smart home use cases to be demonstrated have been selected and reported in a preliminary version of D6.1. Currently Mind, as WP6 leader, is organising a series of developer meetings during which the implementation details of a number of smart home use cases are studied and discussed with all the partners. Currently, we have already studied and discussed workflows and use cases related to the house and user creation process, the joining procedure of smart and not so smart devices, the integration between Yggio and the software components that are going to be executed on the smart devices, the removal of smart and not so smart devices, the procedure to send commands to devices and the integration of the SIFIS DHT and Yggio with the WebThings discovery mechanism.

Task T6.2: Use Case Security and Privacy Goal Refinement (M15-M30/ RIOTS)
The activities of this task have been carried out mainly during the developer meetings organized by Mind. While discussing the different smart home use cases to be considered in WP6, attention has been devoted to analysing the security and privacy aspects of every use case. We are currently defining the trust model of the different use cases and highlighting possible security related issues to be addressed. Also, we have already started discussing in detail how to provide resiliency and network/node failure tolerance to a SIFIS-HOME system. In the next months we are going to define the procedure to install third-party applications on the smart devices and how to integrate the policy manager component.

Task T6.3: Use Case Design and Implementation (M20-M34/ MIND)
Task due to start in M20.

Task T6.4: Experimental Evaluation and Validation (M20-M36/LUM)
Task due to start in M20.

Achievements
During the reporting period, the following has been achieved:

- Preparation of a preliminary version of D6.1 reporting the different devices that are going to be used in the pilot as well as a preliminary list of smart home use cases that are going to be implemented in WP6.
- Development of a preliminary WebThings compliant version of the software managing one of the WiFi actuators used by Mind (Shelly1PM).
- Discussed implementation details with all the partners for:
    - the house creation process

- the user creation process
- the join procedure for a smart device and a not so smart device
- the integration between the software components provided by Yggio and the software components running on the smart devices of the house, regarding data synchronization, management of conflicts, and user database synchronization.
- the removal of smart device and a not so smart device
- the procedure to send commands to a physical device both from an application running on the smart devices and from a remote side
- the integration between the WebThings discovery mechanism and the SIFIS-HOME DHT and Yggio

1.2.7 WP7: Dissemination, Standardization and Exploitation

Objectives (Copied from Annex I - Description of Action)

- Objective 7.1: Develop and maintain the project website, as well as material for project presentations;
- Objective 7.2: Organize training sessions and workshops related to the project's activities;
- Objective 7.3: Ensure an effective dissemination of project results, especially through publications in national and international venues, as well as demonstration platforms and pilots;
- Objective 7.4: Ensure an effective contribution to standardization activities in international bodies;
- Objective 7.5: Ensure an effective planning for commercial exploitation of solutions developed in the project.

Progress per Task

Task T7.1: Dissemination (M1-M36/CNR)
This task has been extremely active in the first 18 months of the project providing contributions on both academic dissemination and engagement of the general public. So far, the main results have been:

(i) Publication of 10 scientific papers, in GII-GRIN-SCIE ranked international conferences and high-to-top quality journals (Q1-Q2 SJR) as well as magazines. The full list of publications is reported in D7.1.
(ii) Publication of the SIFIS-Home website resulting in deliverable D7.7.
(iii) Preparation and management of the social network pages of the project on Twitter, LinkedIn and YouTube.
(iv) Presentation of the SIFIS-Home activities at an online workshop.
(v) Organization of a workshop sponsored by SIFIS-Home to be held in August as satellite event of a cybersecurity conference. For additional details please refer to D7.1. The activities also included the recording and editing of a video of the people involved in SIFIS-Home and preparation of additional dissemination material, such as posters and flyers is currently ongoing. Moreover, two papers co-authored by at least two different partners are being produced as result of the ongoing activities of WP1, WP2 and WP3.

The task has been led by CNR, with a strong participation of CEN for the preparation of the dissemination material and of RISE and POL for the academic publications.

During the first period, FSEC has led the group of partners participating in the creation of SIFIS-Home project presentation video with strong participation of RIO, CEN and CNR. The aim is to publish the video in M19. This forms a continuum to the partner presentation video created at the beginning of the project by expanding the dissemination activities via project communication channels.

Industry partners, with strong participation by FSEC and RIO, have also started the planning of attending potential industrial events for dissemination and exploitation purposes during the second period of the SIFIS-Home project. Evaluation of the potential impact of participation to different events has also taken place.

All project partners have continued the active engagement in various social media communication activities on Twitter, LinkedIn and YouTube, as well as produced blog posts and news material about the ongoing project activities and project progress for the SIFIS-Home website.

Task T7.2: Standardization (M1-M36/ RISE)
The task started in M1 according to plan. Since then, and building on a long-term experience, RISE and Ericsson have been greatly engaged in standardization activities under the international body Internet Engineering Task Force (IETF). These activities have especially targeted the following IETF Working Groups:

- Constrained RESTful Environments (CoRE) [7.2-CORE].
- Authentication and Authorization for Constrained Environments (ACE) [7.2-ACE].
- Lightweight Authenticated Key Exchange (LAKE) [7.2-LAKE].

RISE and Ericsson have participated in the following IETF meetings and respective Hackathons events.

- IETF 109 (November 2020, Online).
- IETF 110 (March 2021, Online).
- IETF 111 (July 2021, Online).
- IETF 112 (November 2021, Online).
- IETF 113 (March 2022, Vienna).

Furthermore, RISE and Ericsson have participated in regular Working Group virtual interim meetings and in official interoperability events aimed at testing implementations of standard proposals.

This has resulted in advancing the status of authored specification documents in the form of Internet Drafts within the Working Groups mentioned above, followed by regular submissions of revised document versions and their presentation at official Working Group (interim) meetings. The standardization proposals documented in such Internet Drafts have been developed by taking as input most of the activities from WP3 “Network and System Security”. The full list of IETF Internet Drafts is available in the project website at [7.2-LIST].

Notably, during this period, four Internet Drafts were adopted as Working Group documents, of which three in the CoRE Working Group [7.2-ADOPTED1] [7.2-ADOPTED2] [7.2-ADOPTED3] and one in the ACE Working Group [7.2-ADOPTED4]. Furthermore, one Internet Draft from the ACE Working Group was approved for publication as Proposed Standard [7.2-APPROVED1].

Finally, Francesca Palombini (Ericsson) got appointed IETF Area Director for the "Application and Real Time" (ART) Area, which includes also the CoRE Working Group among others.

[7.2-CORE] https://datatracker.ietf.org/wg/core/about/
[7.2-ACE] https://datatracker.ietf.org/wg/ace/about/
[7.2-LAKE] https://datatracker.ietf.org/wg/lake/about/
[7.2-LIST] https://www.sifis-home.eu/index.php/standardization/
[7.2-ADOPTED1] https://datatracker.ietf.org/doc/html/draft-ietf-core-observe-multicast-notifications
[7.2-ADOPTED2] https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-edhoc
[7.2-ADOPTED3] https://datatracker.ietf.org/doc/draft-ietf-core-oscore-key-update/
[7.2-ADOPTED4] https://datatracker.ietf.org/doc/draft-ietf-ace-revoked-token-notification/
[7.2-APPROVED1] https://datatracker.ietf.org/doc/draft-ietf-ace-oscore-profile/

Task T7.3: Business Planning and Commercial Exploitation (M7-M36/ FSEC)

The task has been led by FSEC with good cooperation among all partners. All partners have participated in this task and work has started as planned. Task meetings coordinated by FSEC have been part of the

WP7 monthly meetings from the start of the project. During the first period, all partners have reviewed the initial exploitation plans for the project. In addition, planning for the project's exploitation activities started.

During the first period, all partners have continued participation in task meetings led by FSEC as part of the WP7 monthly meetings. As a continuum for the review of the initial exploitation plans for the project that started during the first period, all partners have updated the initial plans and made necessary modifications according to the overall project progress and developments achieved so far as well as preliminary results that can be forecasted at this stage. The content planning and writing work of the deliverable D7.3. Preliminary Business and Exploitation Plan was initiated and completed during the second period with additional meetings every other week for two months dedicated specifically to this deliverable work. An innovative workshop on business scenarios planning was also organized with all WP7 partners attending the session. The detailed results of the workshop are included in the D7.3. report in the section 3. Business Scenarios. The D7.3. report was internally and throughout reviewed by CEN and ERI and based on the review comments, finalized and submitted on time for the M18 deadline.

Industry partners, with a strong participation by FSEC and RIO, have also started the planning of attending potential industrial events for exploitation and dissemination purposes during the second period of the SIFIS-Home project. Increased focus towards the exploitation and dissemination activities of industry partners will follow as the project is approaching the second period with preliminary results. Evaluation of the potential impact of participation to different events, especially from the commercial point of view, has also taken place.

Community building for the project has also started during the first period. The main results have been the participation of SIFIS-Home in some meetings of the WebThings community, where we have highlighted the current lack of some critical security elements and got the interest from the community to include open source components produced in the project to possibly address such issues. The second achievement is CNR becoming the leader of the Working Group on Artificial Intelligence and Cybersecurity in the Italian Association for Artificial Intelligence (AIxIA). This last effort will be used to promote the research activities performed in WP4.

The community building for the project that started during the first period has continued with the following activities engaged by the partners:

WebThings

- Participation to some meetings of the WebThings community.
- Direct discussions with the project leader Ben Francis (Krellian CEO), discussed interest about integration of SIFIS-Home security components into the WebThings framework.

AIxIA (Italian Association for Artificial Intelligence)

- Created a working group on cybersecurity and AI working on WP4 topics. CNR leads the working group.
- Sponsorship of the SIFIS-Home activities in the WG related events.
- Asked to organize a panel on WP4 topics.

Achievements

During the reporting period, the following have been achieved:

- The first deliverable, D7.7 SIFIS-Home Website, was submitted on schedule in January 2021.
- The external communication channels and the visual identity for the project, including the website, social media channels (Twitter, LinkedIn and YouTube), logo and presentation materials, were created and set up in the beginning of the project with active content creation from the start.
- Participation to several IETF general meetings, Working Group interim meetings and related Hackathon /testing events.
- 3 IETF Internet Drafts were adopted as Working Group documents in the CoRE Working Group.
- 1 IETF Internet Draft was adopted as Working Group document in the ACE Working Group.
- 1 IETF Internet Draft from the ACE Working Group was approved for publication as Proposed Standard.
- 6 published Journal articles; 2 published conference papers; 1 published magazine article.
- The deliverable D7.1 Preliminary Dissemination Report was submitted on schedule in March 2022.
- The deliverable D7.2 Preliminary Standardization Report was submitted on schedule in March 2022.
- The deliverable D7.3 Preliminary Business and Exploitation Plan was submitted on schedule in March 2022.
- Active content creation in the external communication channels (SIFIS-Home project website, Twitter, LinkedIn and Youtube) has continued during the second period with 9 blog posts, various news posts, tweets and retweets through the SIFIS-Home project website, project and partner Twitter accounts and LinkedIn account posts about the project progress, ongoing activities, events, milestones and videos presenting project achievements and partner introductions.
- 2 additional scientific journal papers published, 1 white paper published and 3 news journals (Wired IT, RaiNews 24, Sky Italy (Pop Economy) with interviews included created.
- 1 workshop organized (ETAA 2021), 2 workshops participated
- Participation to dissemination event (Internet Festival, Italy 10/2021)
- All technical WPs developed and completed demonstration platforms and pilots to present the preliminary results achieved in the project and these will be utilized for effective dissemination of project results via various communication channels, such as the social media platforms, project website and event participation.

1.2.8 WP8: Project Management

Objectives (Copied from Annex I - Description of Action)

- Objective 8.1: Collate Deliverables, Milestones and Reports;
- Objective 8.2: Manage Legal, Contractual, Financial, Ethical and Administrative Matters;
- Objective 8.3: Ensure Communication between Partners;
- Objective 8.4: Manage Scientific and Technical Activities;
- Objective 8.5: Organise Project Steering Committee.

Project Milestones

The overall progress with respect to the project's milestones due in the reporting period is summarised below.

Milestone	Verification	WP	Due Date	Delivery Date	Comments
MS1 Initial requirement elicitation	This milestone will be considered reached after the first iteration of the requirement elicitation, related to the activities of WP1-4 will be completed and correctly reported in D1.1. These requirements will consider the aspects related to the architecture and the specific technical and technological requirements needed by the activities of WP3 and WP4.	WP1, WP2, WP3, WP4	M6	M6	Deliverable D1.1 submitted on 30/3/21.
MS 2 First architecture and components design	This milestone will be considered reached after the release of the first version of the SIFIS-Home framework is released and published in D1.3.	WP1, WP2, WP3, WP4	M12	M12	Deliverable D1.3 submitted on 30/9/21
MS3 Requirement Refinement	This milestone will be considered reached after the final iteration of the requirement elicitation, related to the requirement elicitation activities of WP1-4, which have been completed and are reported in D1.2.	WP1, WP2, WP3, WP4	M12	M12	Deliverable D1.2 submitted on 30/9/21.

Progress per Task

Task 8.1: Collate deliverables, milestones and reports (M1-M36/CNR)

The activities of this task carried out in the first 18 months have concerned the management of the internal review, formatting and submission of deliverables D1.1, D1.2, D1.3, D2.1, D2.2, D2.6, D3.1, D3.2, D4.1, D4.2, D7.1, D7.2, D7.7, D8.1 and this same report. All deliverables have been submitted on time.

Task 8.2: Manage legal, contractual, financial, ethical and administrative matters (M1-M36/IC)

The main contractual activity executed in this task have been the successful negotiation of a grant amendment to withdraw Mozilla from the consortium and to redistribute Mozilla's responsibilities, tasks and budget among the remaining consortium partners. Notably, the role of project coordinator was transferred from Mozilla to CNR. Additionally, the project's pre-financing grant funds were fully distributed to the consortium partners within the first 1-2 months of the project start.

Task 8.3: Ensure communication between partners (M1-M36/CNR)

The activities of this task in the first 18 months have concerned the setup of the collaboration platforms

to work on the project and ensure regular meetings. The first 18 months of the project have been conducted under the COVID-19 pandemic, hence the set up of collaborative tools such as Git, Github, Gitlab, Miro and HackMD has been of capital importance to have a structured management of all project activities. This task has also handled the organization of plenary meetings, including the kick-off. The plenary meetings have been held partially as fully virtual and partially as hybrid physical/virtual, organized respectively in Turin and Pisa, Italy.

Task 8.4: Manage scientific and technical activities (M1-M36/CNR)
This task has leveraged the experience of the academic partners - especially CNR, POL, CEN and RISE - to ensure that all activities performed up to M18 have been conducted by adhering to standardized methodologies and best practices, with a holistic approach to ensure scientific rigour of the produced material and adherence to software engineering validated procedures for requirement elicitation and architecture design.

Task 8.5: Organise project steering committee meetings (M1-M36/IC)
Project steering committee meetings have been held regularly on the second Thursday of each month except when they have been merged with the three plenary sessions. During the steering committee meetings, each WP leaders has provided a brief status report for their WP and highlighted any particular issues. During the plenary session of 7/6/21, the consortium was joined by the project's Advisory Board.

Achievements

During the reporting period, the following have been achieved:

- Grant amendment successfully negotiated to withdraw Mozilla and redistribute their tasks and budget.
- Project steering committee meetings have been held regularly on the second Thursday of each month.
- Three plenary sessions and one Advisory Board meeting have been held.
- All project deliverables due at M18 have been submitted on schedule.

1.3 *Impact*

The information in Section 2.1 Expected Impact of the DoA is still relevant and currently does not need to be updated.

2 Deviations from Annex 1 and Annex 2 (if applicable)

No deviations are to be reported at this stage.

3 Tasks

Tasks and activities are currently on schedule.