D8.3

Period 2 Management Report

WP8 – Project Management

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 30/09/2023
Actual submission date: 30/09/2023

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

30/09/2023
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 (FSC), Luca Ardito (POL), Andrea Saracino (CNR), Marco Tiloca (RISE), Paolo Mori (CNR) Hakan Lundstrom (SEN), Domenico De Guglielmo (DOMO), Sini Olkanen (FSC), Giles Brandon (IC)

Approved by: Giles Brandon (IC)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	15/12/2022	Defined ToC	CNR, IC	All
0.2	28/01/2023	Third internal report at M27	IC	All
0.3	20/09/2023	Integrated reviewers' comments	CNR	All
1.0	30/09/2023	Submitted Version	IC, CNR	All

Executive Summary

This deliverable reports the progress report for Period 2 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 second half of the project. The project report has followed two iterations: an internal reporting at M27 and a second one at M36.

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.

Summary of the work progress towards achieving the objective: This activity continued between the months 19 and 24. The contribution was culminated in D1.4 that defined and finalized the attributes of the public APIs. The emphasis was to define generic interfaces for the public APIs compatible with high level implementation-independent framework, namely Web of Things and FIWARE. On one hand, the FIWARE interface has a role to enable applications to control the house remotely by exploiting both the Yggio graphical interface and the Ratatosk implementation of FIWARE. On the other hand, Web of Things has been used and extended to offer discover functionalities for applications and services running directly on the smart devices. The activity also resulted a set of workflows and the APIs are building blocks for the defined workflows to matched with the user stories defined in D1.1 and D1.2.

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.

Summary of the work progress towards achieving the objective: This activity has been carried out as core work of WP2. The definitions of metrics for code quality and security have been reported in D2.1 together with a set of best practices for third-party developers to produce reliable applications, reducing thus the attack surface available to attackers. This activity has been carried out in parallel with the definition of labels for safety and potential cyberphysical hazards intrinsically connected to the usage of functionalities of devices with effect on the physical domain. This work has been described in D2.2 and has been integrated, together with the code quality evaluation in a preliminary implementation of developer tools, shown in demoes available through the SIFIS-Home YouTube channel and that will be released in D2.3.

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.

Summary of the work progress towards achieving the objective: As its core work and consistent with its mission, WP3 has continued to carry out the activities relevant to this objective. In particular, research and development activities have been performed by largely building on and exploiting the experience on the following standard technologies: the web-transfer protocol CoAP (RFC 7242); the OSCORE security protocol for protecting CoAP communications end-to-end (RFC 8613); and the ACE-OAuth framework for authentication and authorization (RFC 9200).

Building on the considered background technologies, the activities in WP3 have especially focused on research and development concerning the following topics and security solutions:

i) methods and protocols to ensure end-to-end secure CoAP communications also in group communication setups, with particular reference to the security protocol Group OSCORE and its two modes of operation, namely the group mode and the pairwise mode;

ii) methods and protocols to efficiently establish security keying material between two peers while ensuring crypto agility, flexible authentication and forward secrecy, with particular reference to the key establishment protocol EDHOC and its use for CoAP and OSCORE, as well as to the paired enforcement of fine-grained access control through the standard ACE-OAuth framework and its OSCORE profile;

iii) methods and protocols for provisioning group keying material for the Group OSCORE security protocol in an authorized and authenticated way, as paired with the enforcement of fine-grained access control through the standard ACE-OAuth framework.

iv) methods for enforcing fine-grained, dynamic access and usage control in a single framework, for controlling accesses to remote resources according to adopted access control policies, while contextually establishing/provisioning/updating security keying material and efficiently notifying about early revoked access grants.

The security solutions developed in WP3 have been presented in deliverable D3.3 "Final report on Network and System Security Solutions". Furthermore, the design and development of such security solutions are reflected: i) in the (security) requirements elaborated in deliverable D1.2, as also following and adopting the related feedback received from WP3 and compiled in deliverable D3.1; as well as ii) in the design of the architectural components presented in deliverable D1.4.

The solutions from WP3 mentioned above have been implemented and integrated into the SIFIS-Home testbed and pilot, in concert with relevant partners contributing to WP5 and WP6, and by relying on the process for continuous integration and deployment of Software used in the project. The consolidated description of such a process is provided in deliverable D5.4.

Finally, the solutions developed in WP3 have been input to standardization activities in the international body Internet Engineering Task Force (IETF). Such activities and their results have been reported in deliverable D7.5 "Final Standardization Report".

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.

Summary of the work progress towards achieving the objective: The activities relevant to this objective have been carried out in WP4. At the time of this report, most of the data analytics meant to provide security services to the SIFIS-Home framework have been designed and implemented in Tasks 4.1, 4.2, and 4.4. Such analytics concern the detection of misbehaviours in devices (analysing data or device activity), the detection of children (alone or with adults) in video streams, the detection of network intrusions, and speech recognition. Moreover, the tool for writing and analysing usage policies in order to avoid inconsistency and redundancies has been designed and implemented as well. These analytics have been described in D4.2. In the last period, analytics enabling face and person recognition, anomaly detection, speaker verification and speaker identification have been designed and implemented as well. Moreover, a multilevel intrusion detection analytics, which takes into account information about the device activities gathered all levels of the smart home device stack is being designed, and it will be developed in the next months. The detailed descriptions of such analytics are available in D4.3. For each of these analytics, an analysis of the privacy requirements of the information exploited or produced has been conducted. Moreover, research activities have been conducted to study novel approach to be applied in case of collaborative analytics for properly tuning the parameters of the privacy-preserving mechanisms, and also to choose proper explainability techniques to be adopted, evaluating how they impact each other, and proposing an optimization methodology to have the best possible trade-off among them. The integration of privacy mechanisms, also following the aforementioned strategy, is currently ongoing through the design and development of the Anonymization Toolbox, and it is extensively discussed in D4.3. Relevant research publications (already published and in preparation) on the aforementioned achievements are reported in a separated document.

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.

Summary of the work progress towards achieving the objective: WP5 is focusing on both implement the SIFIS Home test bed and implement and deploy the SIFIS Home architecture as designed by WP1. As stated in D5.2 during this work issues in the original design of WP1 architecture was found which was feedback to WP1 and later corrected in D1.4. The implementation status of the revised architecture is progressing well, every component has an agreed upon owner and if it is not already integrated there is an estimated date when the component will be ready for integration. Some components are considered essential components and gets a higher priority to complete the development of since they are vital to run, deploy and verify the overall architecture. Regarding the SIFIS Home test bed so as stated in D5.1 will part of it be executed on the CNR Panarea server complemented with live SIFIS Home devices. The definition of the test bed is now completely agreed upon and every part of it to finalize it has an assigned owner. A key item is how to handle the simulated devices and it was decided each will be executed in a Docker environment in separate virtual machine on the Panarea server. So far only mostly unit test of the different components one by one has been done since not all essential components ready for integration integrated yet.

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 DOMO 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.

Summary of the work progress towards achieving the objective: The initial activities of WP6 focused on defining a set of smart home use cases, highlighting their functional and performance requirements. Also, we identified the set of physical devices to be used in the WP6 pilot. The set of use cases to consider and the devices that we planned to use have been initially reported in D6.1 and then refined in D6.3. Then, we focused on developing a physical smart home testbed, composed of different devices using the SIFIS-HOME framework, to implement and test the proposed smart home use cases. The initial implementation of the WP6 testbed has been presented in D6.2, while D6.4 describes all the details of the final pilot implementation and the results of the use cases validation. The WP6 pilot is composed of both Smart (SD) and Not so Smart devices (NSSD). In detail, the testbed uses DoMO Gateways and standard amd64 Laptops as Smart devices while the DoMO WiFi actuators are the Not so Smart Devices that we considered. The specific technical activities that we performed are summarized in the following and are reported in the WP6 deliverables.

- Web of Things Firmware implementation for the DoMO WiFi actuators: the NSSD devices being part of the pilot need to expose a Web of Things compliant API. In detail, in a WoT-based architecture every NSSD is a server that exposes a set of functionalities to possible clients. Web of Things does not mandate the use of a specific protocol to make the functionalities of a Web Thing accessible to an external application. In our implementation, we decided that our NSSDs are HTTPS servers exposing their functionalities through a WebSocket API. In a WoT server properties are used to expose settings and characteristics of a WebThing. For example, we can have a property description that is a textual description of a certain WebThing (e.g., “kitchen light”). In addition, actions are used to request the execution of a certain operation to a WebThing. A possible action to allow a user to turn on and off a certain light can be, for example, "turn". Web of Things also provides events to allow a WebThing to signal anomalous conditions. The WoT firmware for the DoMO WiFi actuators has been developed using the C++ language and the Arduino Framework. We also used PlatformIO (https://platformio.org/) to simplify the firmware development and building processes. The WiFi actuators that our firmware supports are the Shelly 1, Shelly 1PM, Shelly 2.5, Shelly RGBW, Shelly Dimmer and Shelly EM. Also, our final firmware implementation supports the Shelly 1 Plus devices that also have Bluetooth connectivity and allow to receive information from Bluetooth sensors and actuators that are in their proximity.
- OpenWrt SIFIS-HOME distribution for the DoMO gateway: The DoMO gateway is a quite powerful device, based on the Banana PI R3 board, that is provided with a Quad Core ARM A53 CPU and 2 GB of DDR RAM. Also, it has 8GB of EMMC flash available and is equipped with a 500 GB NVMEe disk. Regarding network connectivity, the DoMO gateway is equipped with two 4x4 WiFi 6 network chips (2.4Ghz and 5Ghz bands), 5 Gb Ethernet ports and 2 2.5 Gb SFP ports. Also, it is provided with a user-accessible USB 3.0 compliant port that allows connecting external USB devices. The DoMO gateway runs an OpenWrt Linux distribution. We prepared a specific OpenWrt distribution for the DoMO gateways that includes the various components that are needed to execute the SIFIS-HOME software components to be used. In detail, such distribution contains the docker and docker-compose packages allowing the DoMO gateways to execute all the required SIFIS-HOME components. We prepared a simple bash script that automates the whole SIFIS-HOME OpenWrt image creation Docker images: we prepared specific GitHub actions that allow building the different SIFIS-HOME components for both arm64 and amd64 architectures. We also prepared a dedicated Docker Image for every SIFIS-HOME component that has been used and integrated in the WP6 pilot.

- Docker-compose files: we prepared a docker-compose file that is used on both the DoMO gateways and the pilot Laptops. The docker-compose file contains the list as well as the configuration of all the SIFIS-HOME services that should be executed on a SD.
- Integration: as mentioned above, all the different SIFIS-HOME components are available as dedicated Docker images. We integrated all of them in the pilot and tested that they operate correctly when executed on the pilot physical devices.
- Use cases validation: we validated 19 different smart home use cases using our pilot. The validation we performed is described in detail in D6.4. Also, a demo video for each one of them has been prepared.
- VPN server and VPN manager implementation: we developed a technical solution that uses i) a VPN server, ii) a VPN client and iii) a nginx proxy server, that makes services running on the SDs accessible from a remote side. In detail, it makes the DHT Manager web service, the privacy dashboard panel and the policy translation point panel running on a SD deployed in the house available from a remote side.
- Fiware API component implementation: this component forwards the persistent messages published through the DHT to the Ratatosk FIWARE Context broker that is part of the Yggio instance residing on the SIFIS-Home cloud. Also, it forwards commands entered by the user in the Yggio user interface to the DHT.
- Mobile application implementation: the Mobile Application allows users to easily manage the SIFIS-Home network basic functionalities. This includes listing the installed devices within the home, enabling users to perform various actions on these devices, such as collecting environment measure readings, or controlling actuators, or turning devices on or off. Additionally, the Mobile Application provides access to system logs for monitoring purposes, as well as the ability to install third-party applications directly into the SIFIS-Home framework, in order to extend the capabilities of the system. The Mobile Application was written in Javascript and Vue utilizing the NativeScript framework and the Stackblitz development environment.
- domo-bootstrap: we developed a Web server application, that runs on the DoMO gateways composing the pilot, that offers an API through which it is possible to initialize new Smart Devices. In particular, the application allows a Smart Device to receive all the information it needs to join a SIFIS-HOME network.
- domo-scheduler implementation: the role of the domo-scheduler is to elect one *leader* device among all the different SDs that are present in a certain SIFIS-HOME network, in a dynamic way. The leader device is the only one allowed to execute specific services of the smart home, that are named *cluster* services.
- SIFIS-SD-nginx-server implementation: it is a nginx proxy server that is used to protect the web services running on the SDs from external access.
- SIFIS Light Manager: such component takes care to turn on and off the physical lights of a certain room when the physical buttons of the room are pressed/released by the users of the smart home.
- SIFIS-HOME DHT Manager: The SIFIS-HOME DHT is a component that offers a completely distributed publish/subscribe mechanism through which SIFIS-HOME applications can exchange messages. The SIFIS-HOME DHT allows to publish both persistent and volatile messages. Persistent messages are messages that need to be stored in a persistent way, so that they are available even after a node reboot operation. In detail, persistent messages are stored on an Sqlite database. Volatile messages are instead messages that need to be delivered to all the available applications but that do not need to be persisted on disk. The SIFIS-HOME DHT has been developed using the Rust language. Rust applications can include the DHT by embedding it as a library. Non-Rust applications can access the DHT by means of a REST + WebSocket API provided by the DHT Manager.
- SIFIS-HOME NSSD Manager: The SIFIS-HOME NSSD Manager is the SIFIS-HOME component responsible for interacting with the NSSD devices present in the house. It has been developed using the Rust language and is composed of three main modules: the DHT module, the M-DNS Module and the Web of Things (WoT) Module.

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.

Summary of the work progress towards achieving the objective:
During the reporting period, SIFIS-Home partners have further strengthened the dissemination and communication activities via the established social media platforms (Twitter, LinkedIn and YouTube) and project website following the strategy for publications and events participation and organization, in line with the project DoA. During the project, the website has attracted over 37k visitors and 85k visits in total, Twitter gained more than 120 followers with approximately 750 tweets, LinkedIn more than 60 followers, YouTube channel with 16 videos and more than 360 viewers in total. Consortium has published 20 blog posts and 16 news articles to the project website. Furthermore, partners have published in 10 journal publications, organized and participated in 7 academic conferences or workshops and attracted attention in news channels and magazines. The consortium has focused on the industrial dissemination and exploitation, by taking part in 23 industrial events, including key international conferences and seminars, with keynotes and other presentations. Further details of the above can be found in the sections 2.1 and 2.3 of this document and the D7.4 and D7.6.

The consortium has worked on community building activities by cooperating with WebThings and subsequently with the W3C Web of Things (WoT) standardization group, to make the extensions related to hazard representation and developer guidelines available. This cooperation with W3C WoT and the publication of developer tools from SIFIS-Homepave the way towards a community of security-aware developers of Smart-Home applications. Moreover, as part of the activity to contribute back to the opensource organizations maintaining software we leverage, we are contributing back to the Rust and OpenWRT communities bugfixes and improvements.

Standardization activities have been carried out through the contribution of SIFIS-Home partners to the premier international standardization bodies Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). The deliverable D7.5 "Final Standardization Report" describes the activities and results within those organizations, as well as how such organizations operate and their process.

With respect to the IETF, this has consisted in RISE and Ericsson co-authoring RFCs and Internet Drafts as technical specifications, participating to related implementation interoperability tests, and attending regular IETF meetings as well as Working Group interim meetings. In particular, the solutions and methods developed in WP3 have been the main input for several, regularly revised Internet Drafts within the IETF Working Groups ACE, CoRE, LAKE and SCHC. As per IETF procedures, such Internet Drafts have undergone a complex assessment process including in-depth reviews and analysis. One of those has been published as RFC 9203 (Proposed Standard), publication has been approved for one of them as Proposed Standard RFC, publication has been requested for 4 of them as Proposed Standard RFCs, and most of them are adopted as Working Group documents, i.e., there is a formal community commitment to collectively work on those towards their publication as a standard. Additional duties are also undertaken within the IETF, with individuals from the engaged partners acting as Area Director for the Application and Real Time (ART) Area, Working Group Chair for the CoRE Working Group, member and reviewer in the IoT Directorate, as well as reviewer for the ART Area Review Team.

With respect to W3C, Luminem has been involved in the W3C Web Of Things (WoT) Community, where it is now a full-fledged member and has been active within the WoT Interest Group, Community Group and Working Group. The contribution in W3C WoT is related to the activities carried out in WP2, and concerns the overhaul of the Thing Description 2.0 information model, in particular regarding the WoT-Profile and the Protocol Bindings Templates to address the concerns on describability, ultimately to ensure semantics interoperability of the used information models. Furthermore, Luminem has contributed with a from-scratch Rust implementation of WoT standards, also integrating the SIFIS-Home Risk/Hazard labels in simulated things, of which it has also authored a related use-case document.

Exploitation and business planning activities have focused on providing further insights to the D7.6 business and commercial exploitation planning, including the analysis of Key Expoitable Results (KERs) of the project and their exploitation and impact potential, as well as a specific business and exploitation plan for the main result of the project, the SIFIS-Home Framework, including sustainability and monetizing plans. Furthermore, partners have updated and elaborated their individual exploitation plans to ensure effective exploitation of the solutions developed in the project. The consortium also participated in a joint dissemination and exploitation event with other 4 projects funded by the same call in the IoT Solutions World Congress and Cybersecurity Congress held jointly in Barcelona 31.1.-2.2.2023. The event served as a key dissemination and exploitation activity for the project, as the SIFIS-Home project showcasedpreliminary results and demonstrations at a shared exhibition booth and stand with daily presentations. The activity offered an opportunity to receive feedback from potential end users and customers. The project partners also published a joint press release about the event. In addition, especially the industrial partners have participated in 23 industrial events to showcase the project to potential end users and customers within the target markets. Further details of the events are described in the section 2.3 of this document.

Overview of the project objectives per WP

Objective	M36 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.	Completed
▪ Objective 1.2: Elicit architectural functional and non-functional requirements to ensure the functionality of a smart home architecture.	Completed
▪ Objective 1.3: Define privacy and security goals for the SIFIS-Home Security Architecture to effectively improve resilience of smart home systems.	Completed
▪ Objective 1.4: Design prescriptive components for the SIFIS-Home Security Architecture to accommodate functional and security requirements.	Completed
▪ Objective 1.5: Design the whole SIFIS-Home Security Architecture, defining component interaction, interconnections and operative workflow.	Completed
▪ 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.	Completed
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	Completed
▪ Objective 2.2: Define privacy metrics for evaluating the infrastructure	Completed
▪ Objective 2.3: Deliver proof of concept of tools which evaluate software	Completed
▪ Objective 2.4: Design guidelines that help developers for writing IoT software	Completed
▪ Objective 2.5: Define policy-based software security compliance	Completed
▪ Objective 2.6: Analyse GDPR compliance, licensing compliance and ethical aspects	Completed
▪ Objective 2.7: Trigger and support dissemination, and exploitation of metrics, guidelines and policy in WP7.	Completed
WP3 – Network and System Security *(WP Leader: RISE)*	

Objective	M36 Achievement
▪ 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.	Completed
▪ 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.	Completed
▪ 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.	Completed
▪ Objective 3.4: Build on the specification and requirements for the distributed system architecture from WP1, and provide feedback for their refinement.	Completed
▪ 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.	Completed
▪ Objective 3.6: Trigger and support the integration of the developed security solutions within the smart home use case undergoing demonstration in WP6.	Completed
▪ Objective 3.7: Trigger and support dissemination, standardization and exploitation of developed solutions in WP7.	Completed
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.	Completed
▪ 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.	Completed
▪ 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.	Completed
▪ 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.	Completed
▪ 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.	Completed
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.	Completed
▪ 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.	Completed
▪ 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.	Completed
▪ 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.	Completed
▪ 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.	Completed
WP6 – Smart Home Use Case *(WP Leader: DOMO)*	
▪ Objective 6.1: Deploy the SIFIS-Home framework in the Mind architecture to implement the use case.	Completed
▪ 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.	Completed
▪ 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.	Completed
WP7 - Dissemination, Standardization and Exploitation *(WP leader: FSEC)*	
▪ Objective 7.1: Develop and maintain the project website, as well as material for project presentations.	Completed
▪ Objective 7.2: Organize training sessions and workshops related to the project's activities.	Completed

Objective	M36 Achievement
▪ 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.	Completed
▪ Objective 7.4: Ensure an effective contribution to standardization activities in international bodies.	Completed
▪ Objective 7.5: Ensure an effective planning for commercial exploitation of solutions developed in the project.	Completed
WP8 – Project Management *(WP Leader: IC)*	
▪ Objective 8.1: Collate Deliverables, Milestones and Reports	Completed
▪ Objective 8.2: Manage Legal, Contractual, Financial, Ethical and Administrative Matters	Completed
▪ Objective 8.3: Ensure Communication between Partners	Completed
▪ Objective 8.4: Manage Scientific and Technical Activities	Completed
▪ Objective 8.5: Organise Project Steering Committee	Completed

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)
This task was completed in Period 1.

Task T1.2: Security and Privacy Goals (M3-M12/CNR)
This task was completed in Period 1.

Task T1.3: Definition of Secure Component Design, System Architecture, and Intercommunication (M6-M24/FSEC)
The task continued the work between M19 and M24 according to the plan. The focus in T1.3 was on the design of the SIFIS-Home Security Architecture, defining components, functionalities, interconnections and operative workflows. This task contributed to D1.4 which had a deadline in M24.

The architecture design was carried out during “hands-on” telco calls. During the pandemic, we started to use telco meetings and collaborative methods to design the architecture. We continued to use a tool called Miro (https://miro.com/) to carry out collaborative design in real-time. This task also worked in co-operation with T1.4 and WP5 and organizing joint bi-weekly meetings. Accordingly, the details of the SIFIS-Home architecture and framework are presented in the next task progress report (Task 1.4). Deliverable 1.4 was submitted on time at M24.

Task T1.4: Definition of Secure Development APIs (M6-M24/POL)
Regarding task 1.4, between M19-M24 effort has been spent in the extension of the set of secure development APIs, that were built on top of the results of the tasks reported in deliverable 1.3.

A final architecture of the SIFIS-Home framework has been described with the objective of complementing and correcting the preliminary architecture described in deliverable D1.3. The architecture has been designed by adopting a modular, microservice-based architecture, where each component offers a specific set of functionalities that can be invoked either by other architectural components or externally. The high-level infrastructure comprises five major components, namely the Smart Device Framework, the Application Framework, the NSSD Framework, the Cloud Framework, and the Development Tools. All the components of the architecture are detailed in section 3 of deliverable 1.4.

The definition of the architecture involved the finalization of the design of the DHT (Distributed Hash-Table) and allowing access to the DHT to all the other components. The Publish/Subscribe DHT software component is a software module that allows communication among SIFIS-Home software components and SIFIS-Home devices using a publish/subscribe pattern, whilst providing an easy-to-use mechanism to share information among

devices and applications. Details about the implementation and reference scenarios of usage of the DHT are reported in section 3.1.7 of deliverable 1.4.

On top of the re-defined SIFIS-Home architecture and communication means between different components, the activities between M19 and M24 entailed the definition of the APIs exposed by each component of the SIFIS-Home architecture. The defined APIs belong to two different categories: application APIs, used by the home control application and the configuration portal, and defined as REST APIs, and Internal APIs, used by the SIFIS-Home architecture components as a means of internal communications and defined as SDKs. All the REST APIs belonging to the first category were described by utilizing the OpenAPI specification, which is the de-facto industrial standard to define REST based APIs. The definition of such OpenAPI specification, documented through the Swagger Editor, has been reported in its entirety in appendix A of deliverable 1.4.

Finally, the main utilization scenario of the SIFIS-Home application has been documented in the form of operative workflows, in terms of calls to the secure APIs previously defined. The ten different main workflows of the SIFIS-Home system are reported in section 6 of deliverable 1.4.

Contribution per partner to WP1

Partner	Contribution
CNR	Participation in WP1 meetings, contribution in the definition of API, design of the threat model, workflow definition.
ERI	Regular participation in WP1 meetings and contribution to the SIFIS-HOME architecture.
FSEC	FSEC has been the leader of the WP1 and coordinated the periodic meetings. FSEC has been editor of D1.4. FSEC has also provided contribution to define and revise the SIFIS-Home architecture and requirements.
DOMO	Regular participation in WP1 meetings and contributed to the design of the SIFIS-HOME architecture. Co-authored the released deliverable D1.4
RIO	Participation in WP1 meetings, contribution to the SIFIS-HOME architecture.
SEN	Regular participation in the joint WP1 and WP5 meeting and have actively contributed to the SIFIS Home architectural design as well as use case diagrams. Reviewed D1.4 and wrote some parts of it related to SENS contributions.
RISE	Regular participation in WP1 design meetings; provided analysis, feedback and input on the SIFIS-Home architecture components, based on the development of security solutions in WP3; co-authored the deliverable D1.4.
POL	POL had been the leader of Task 1.4 concerning the definition of secure development APIs. POL had been deeply involved in the activities of WP1, contributing to both the requirement elicitation phase and the SIFIS-Home framework architecture definition.

Achievements

During the reporting period, the following have been achieved:

- WP1 has been a contributor to milestone M5;
- The final version of the SIFIS-Home architecture and SIFIS-Home framework have been released and published in D1.4 on time at M24;
- All the WP1 partners 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 "Guidelines for IoT Software Development and definition of Security and Privacy Metrics" aimed to provide developers with a set of guidelines and metrics for measuring the quality and security of source codes and binaries produced in the SIFIS-Home project or by third-party developers developing apps expected to run on the SIFIS-Home framework. The task focused on evaluating a set of regulations and related measures to analyze privacy implications based on data management strategies with the main goal of implementing applications according to their best security and quality criteria.
As part of this task, two innovative static metrics were created: WCC Plain and WCC Quantized. Both metrics were based on weighted code coverage, a concept that merges code coverage and code complexity together using weights. The main goal of these metrics was to identify parts of source codes that are complex to understand and maintain and, at the same time, partially or completely not tested. The difference between WCC Plain and WCC Quantized is in the weights, plain version does not assign a weight to the complex part of a code.
In addition to these metrics, the task also provided developers with software verification and evaluation tools to assess and communicate the overall quality of source code and produced applications to end-users in a user-friendly way.
The task was successfully completed in M24, providing developers with the necessary guidelines and tools to develop secure, high-quality IoT applications. All the results obtained can be found in D2.1, D2.2, and D2.4.

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

Task 2.2 Dynamic Code Quality/Security Evaluation started at M12 and will be concluded at M30. It integrates static analysis, code coverage, code clarity, and sanitization software techniques to evaluate the IoT software produced by third-party developers of the SIFIS-Home framework. At M24, the team successfully produced the deliverable D2.3 titled "First Version of Developer Tools", which described the main contributions of this task to the SIFIS-Home project. The following paragraphs will summarize such contributions and show the activities carried out from M24 to M29 that are not included in D2.3.

This task defines a series of workflows to evaluate the quality and security of a software. Each workflow is composed of a list of tools which can check for the presence of memory leaks and other vulnerabilities in the final binary through programs such as Valgrind and Asan, some undefined behaviours for the Rust program through Miri, and some security issues through fuzzing techniques.

In order to test the validity of the best practices selected an implementation of the Web of Things standards had been implemented in Rust and used to prepare simulated devices and behavioural testers. As focus project we analysed a crate we would depend on and found the mistakes and corrected them. Being a twice orphaned crate we took maintainership of it and started to send patches to the users of the former crate so they will not have to address the same issues.

During the defined period, three tools have been developed to cover the creation of the workflows, the weighted code coverage metrics, and the snippets of complex code. Sifis-generate generates either new projects for some

build systems or the defined workflows as Continuous Integration scripts with the use of templates. Templates define the layout for a project and allow developers to insert data at runtime. Each template contains all the files necessary to build a project with a build system.

Weighted Code Coverage implements WCC plain, WCC quantized metrics, in addition to two others related to the weighted code coverage concept. It allows users to define thresholds for the complexity algorithms, set up the granularity between files and functions, and the number of threads necessary to parallelize the various tasks, speeding up the computation. It also offers the possibility to define the output.

In the last part of the reporting period, from month 24 to 29th, an additional workflow has been added. This workflow implements a standardized method defined by FSF for declaring copyright and licensing for software projects: REUSE. The REUSE method consists of a set of files that specify the copyright and licensing information of the software. This workflow also provides a comprehensive license compliance report, which provides an overview of the licensing information for all the components of the software project.

Task T2.3: Policy-based Software Security Compliance (M12-M30/CNR)
This task has been dedicated to the definition of tools and methodologies to evaluate security and safety aspects of the third-party applications distributed through the marketplace and installed in the SIFIS-Home framework. The task is focused on defining in a computable manner the level of risk for different aspects of security, privacy and safety. In the first months of SIFIS-Home, this task has defined an ontology to map security, privacy and safety risks according to functionalities exposed by smart and not so smart devices. The ontology exploits the JSON language to define and quantify risks connected to actions and device properties. In collaboration with the other tasks, these functionalities have been defined as abstract and device-agnostic functionalities, then formalized as SIFIS-Home development APIs. To each API a specific risk set is assigned by using the aforementioned ontology. Then, the SIFIS-Home development APIs have been integrated into Web of Things by linking the generic APIs (e.g., turnOnLamp()) with setting of specific values for Things Description properties (e.g., Lamp.status = On).

Through the integration between WoT Thing Descriptions and SIFIS-Home Development APIs, we have assigned a risk level also to specific configurations of entire sets of Thing Descriptions, representing the set of devices in a smart home instance. Through this analysis it is possible to calculate the actual risk that an application installed in a specific smart home instance would actually imply. In fact, analysing the risk of an application at developer's side is done by maximizing the possible risk that an application would pose to a house with the most dangerous configuration, knowing the set of devices present in a house and their description, the risk can be precisely evaluated. For example, an application able to invoke the API openFaucet(), implies a risk of "Flooding" only if the house where it is installed includes a smart faucet answering to that API. The risk level is computed at compilation time and made available to the developer both as deployment agnostic value and compared to a set of standard smart home templates. On the other side, at deploy time, the set of used SIFIS-Home development APIs is extracted directly from the application binary, then the risk is actually evaluated with the house configuration. At this stage, the application is also evaluated against user defined policies, related to privacy, security and safety requirements (e.g., "Do not install application with flooding risk").

Once an application has been deployed, the last element of this task plays its role together with components from WP3 and WP5. In particular, the SIFIS-Home development APIs provide the functionality of a Policy Enforcement Point (PEP) for the Usage Control paradigm. The policies might concern risk mitigation for security, privacy and safety, or limitation of behaviours according to context conditions. Policies are evaluated by the Policy Enforcement Engine component, combining attributes from the application, users' preferences, current home status based on environmental conditions, device status and other applications. A PERMIT decision means that the API invocation can be performed, whilst a DENY decision forces the SIFIS-Home API to terminate without performing actions.

This approach for application policy evaluation and enforcement falls in the set of the Contract-based security methodologies and is derived as an optimization of the Security-by-Contract approach. In particular, the application A is linked to a contract C or manifest describing the behaviour of the application. The level of behaviour representation comes from the set of invoked SIFIS-Home API and their related risk. On the other hand, the policy P is written in XACML and provided by the user. The evaluation is performed at deploy time,

converting the manifest (contract) in an XACML request which is then evaluated as an Access Control policy. The compliance between the application behaviour and contract A ⊨ C is ensured by the automated derivation of the API sets from the source code or binary. The contract-policy matching C ⊨ P is performed through the policy enforcement engine, which is an XACML policy evaluation engine. The final results of this task have been presented in D2.4, providing a fully integrated workflow that goes from policy definition performed through the Policy Manager and then interfaced with WP5 components, in particular the Policy Enforcement Engine.

On the overall, the activities of this task in the period covered by this report can be summarised as follows:

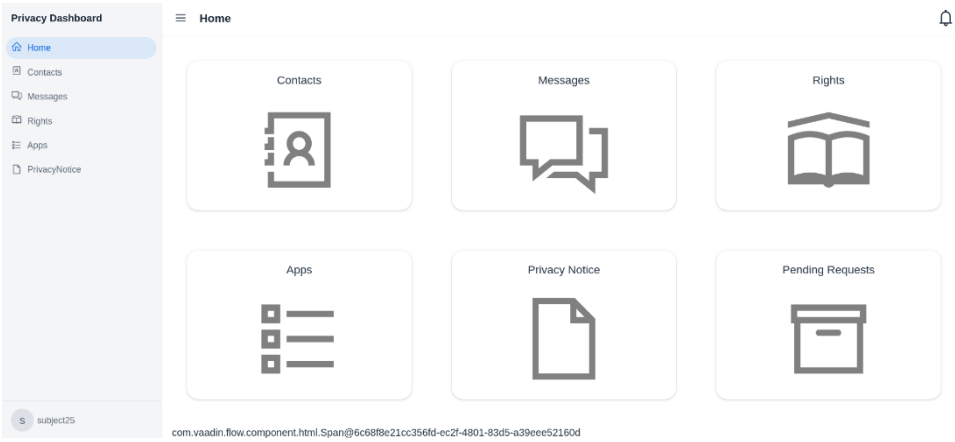
- Integration of the risk ontology with other WP2 components, to make it integrated element of the third-party application development tools.
- Integration of the third-party development APIs with the policy enforcement engine logic, by implementing the inlining of the APIs to generate XACML requests.
- Integration of the Policy Enforcement Point logic (external component of the Policy Enforcement Engine) in the installation process to verify that the installation of an application is compliant with smart home defined policies.
- Development of the SxC logic implemented through the Policy Enforcement Logic, following the definition of Installation Policies and Runtime Policies, mapping respectively the C ⊨ P and the A ⊨ P functionalities.
- The integration of the policy translation point with the Policy Manager to have policies in XACML format.

Task T2.4: Legal Aspects and GDPR Compliance (M1-M30/POL)

Task T2.4 titled "Legal Aspects and GDPR Compliance" focuses on integrating legal and ethical aspects into the guidelines and tools developed within WP2. It supports the design of a list of labels that comply with the GDPR, evaluates the possibility to include labels that allow users to share personal data under certain conditions, creates tools to easily create privacy information, consent and privacy pledges, and adopts policies to foster compliance with license obligations.

The activity performed during the reported period focused on the following topics: design of the Privacy dashboard described in D2.6 (pp. 27-30), update of the ethical analysis framework described in D2.6 (pp. 24-26), work on procedures and tools for free software/open-source licenses compliance, and work on privacy compliance and ethical analysis of pilots.

Starting from M19, the Privacy dashboard is being designed and developed, and technical characteristics are being implemented (e.g., inclusion of APIs). The ethical analysis is being updated, considering also suggestions from reviewers. The procedures and tools concretely used in the development of the SIFIS home technology are being identified and mapped, and support is being provided to pilot developers. The results will be detailed in D2.7 (Final Report on Legal and Ethical Aspects), which will update D2.6 (Initial Report on Legal and Ethical Aspects). The following picture shows the homepage of the Privacy Dashboard under development.



Contribution per partner to WP2

Partner	Contribution
CNR	CNR has participated regularly to the activities of WP2 and led the activities of Task 2.3. In particular CNR has led the activity of ontology definition and risk modelling, supporting the activities of LUM in the integration with WoT. Furthermore, CNR has led the definition of methodology to verify policy compliance of applications and supported the integration with POL tools and the technological results from and toward WP3, WP4 and WP5.
FSEC	Participated in WP2 meetings and applied the proposed guidelines and tools in activities within WP4 and WP5.
LUM	Wrote a WoT implementation in Rust and used it as testcase for the developer guidelines and the tools developed within the WP2 (sifis-generate and weighted-code-coverage)
DOMO	Followed the WP2 activities. Provided feedback to LUM and POL on the usage of the *sifis-generate* tool. Provided support to POL for integrating the Policy Translation Point and the Privacy Dashboard in the project pilot.
RISE	Followed the WP2 activities and its guidelines/principles on code quality and documentation, when working on the automated integration and deployment of security solutions from WP3.
POL	POL is the leader of the WP2 and coordinated the periodic meetings and developments. POL has been editor of D2.1, D2.2, D2.3, D2.6, D2.7. POL has also provided contribution to define and revise the Guidelines for IoT Software Development.

Achievements

During the reporting period, the following have been achieved:

- Implemented and maintained new developer tools (weighted-code-coverage, sifis-generate).
- Contributed to opensource developer tools we rely on (grcov).
- Validated the best practices, their enforcement and the toolset using the wot-rust development as testbed.

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)
This task designs and develops security solutions for securing device operations, interactions and communication. Its focus is especially on methods and protocols to provide robust, end-to-end security of exchanged network messages. Activities on this topic largely take as main building blocks two standard protocols for the IoT, namely the web-transfer protocol CoAP (RFC 7252) and the secure communication protocol OSCORE (RFC 8613).

During the period covered in this technical report, progress has been made in advancing and improving the security protocol Group OSCORE, in order to efficiently ensure end-to-end secure CoAP communications in group communication setups through two modes of operation, namely the group mode and the pairwise mode. Particular focus and effort were put in: strengthening the security properties of the protocol; improving means for asserting and achieving freshness of protected messages; improving the secure handling of multiple responses from the same origin to the same request message; and enabling the discovery via web-linking of resources whose access has to be protected with Group OSCORE.

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

Task T3.2: Security Lifecycle Management (M3-M33/RISE)
This task designs and develops security solutions that 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 work on these topics largely takes as main building blocks the standard protocols for the IoT, namely the web-transfer protocol CoAP (RFC 7252), the secure communication protocol OSCORE (RFC 8613) and the ACE framework for authentication and authorization (RFC 9200).

During the period covered in this technical report, progress has been made especially on the following topics.

- Development of a method for distributing security keying material for OSCORE security groups, as entrusted to a responsible Group Manager and paired with fine-grained access control based on the ACE framework and enforced during the group joining operations.
- Development of the authenticated key establishment protocol EDHOC, with particular advancements in terms of compact encoding of peer identifiers, increased number of encrypted information, improved

support for embedded External Authorization Data, and use for CoAP and OSCORE also by means of an optimized workflow.
- Development of an efficient and automatable method for notifying about early revoked access grants in the ACE framework, through two possible modes of operations of different granularity, namely a full query mode and a diff query mode.

The main design partners involved in this task have engaged in several, regular technical discussions and have effectively progressed the design and development activities according to plans. Task T3.2 is tightly related to Task T3.1, as the respectively developed security solutions are closely related and serving each other. However, since the start of the two tasks, their relation 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)
This task focuses 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 evaluation of access policies.

During the period covered in this technical report, progress has been made especially on the following topics.
- Provided feedback and contributions on appropriate methods for evaluating security policies applicable to applications and network communication.
- Finalized the harmonious integration of access and usage control as both enforced within the ACE framework for authentication and authorization, while also leveraging the (automated) notification of revoked access grants. Such an integrated, enhanced framework has also undergone an extensive assessment and evaluation.
- Defined sets of access control and usage control policies for integration with the activities of Task 2.3.

Furthermore, the main design partners involved in this task have engaged in several, regular technical discussions and are effectively progressing the design and development activities according to plans.

Overall, during the period covered in this technical report, the activities in the three tasks above have focused on the following points.

- Progressing and finalizing the design and development of the security solutions in the scope of WP3. This has advanced the work previously documented in deliverable D3.2 "Preliminary report on Network and System Security Solutions" (March 2022), and resulted in the updated presentation of the outcomes of WP3 activities in deliverable D3.3 "Final report on Network and System Security Solutions" (June 2023), which obsoletes D3.2 and has contributed to the achievement of the Milestone MS7 "Final implementation and deployment of the architecture" (June 2023).
- Providing WP1 with analysis, feedback and input on the SIFIS-Home architecture components, based on the development of the WP3 security solutions. This contributed to achieve the Milestone MS5 "Final component design and first implementation" (September 2022), as per the submission of deliverable D1.4 "Final Component, Architecture, and Intercommunication Design".
- Active engagement in WP5, by producing and executing a plan for integrating security solutions from WP3 into the SIFIS-Home testbed and pilot, in concert with relevant partners contributing to WP5 and WP6, and by relying on the process for continuous integration and deployment of Software used in the project. This contributed to achieve the Milestone MS5 "Final component design and first implementation" (September 2022) as per the submission of deliverable D5.2 "First version of SIFIS-Home Security Architecture Implementation", and the Milestone MS7 "Final implementation and deployment of the architecture" (June 2023) as per the submission of deliverable D5.4 "Final version of the SIFIS-Home Security Architecture Implementation".

As shortly mentioned in deliverable D3.3, WP3 has also carried out research and development activities on some further, in-scope security solutions that, due to time constraints and prioritization choices, have not reached a maturity level that could enable their integration in the SIFIS-Home testbed and pilot. Nevertheless, such topics have fruitfully contributed to dissemination, publications, and standardization activities.

Contribution per partner to WP3

Partner	Contribution
CNR	CNR contributed to the activities of WP3 by working on the integration between the Usage Control paradigm used for policy enforcement, with the ACE technology provided by RISE. CNR has thus led the activities of T3.3 for development of the SIFIS-Home component Policy Enforcement Engine.
ERI	Design, development and analysis of security protocols and enablers in the scope of Tasks T3.1 and T3.2. Driving development of lightweight security handshake and authorization framework profiles.
FSEC	Following and participated in WP3 activities and shared information with WP1 activities.
DOMO	Followed the WP3 activities. Organized dedicated meetings with RISE focused on the development of the CoAP Manager component.
SEN	Following and participated in WP3 activities and provided technical assistance how to enable smooth integration of WP3 solutions in the overall SIFIS Home security architecture.
RISE	Enforced leadership of WP3, and of its tasks T3.1 and T3.2; performed design, development and implementation of network & system security solutions in the scope of WP3; provided WP1 with analysis, feedback and input on the SIFIS-Home architecture components; co-authorship and main responsibility of the deliverable D3.3.

Achievements

During the reporting period, the following have been achieved:

- Progressed and finalized the design and development of the security solutions in the scope of WP3. These especially include: i) methods and protocols to ensure end-to-end secure CoAP communications also within groups, with particular reference to the security protocol Group OSCORE and its two modes of operation, namely the group mode and the pairwise mode; ii) methods and protocols for establishing and provisioning security keying material, with particular reference to the key establishment protocol EDHOC and its use for CoAP and OSCORE, as well as to the paired enforcement of fine grained access control through the standard ACE-OAuth framework and its OSCORE profile; iii) methods for the (automatic) notification of revoked access grants in the context of the standard ACE-OAuth framework; and iv) seamless integration and enforcement of access control and usage control in a single framework.
- As one of the relevant Work Packages, WP3 has contributed to the achievement of Milestone MS5 "Final component design and first implementation", which was achieved on M24 through the submission of deliverables D1.4 and D5.2. To this end, WP3 produced a plan for integrating its security solutions into the SIFIS-Home testbed and pilot, and started to work according to such a plan in concert with relevant partners contributing to WP5 and WP6.
- The third deliverable of WP3, namely D3.3 "Final report on Network and System Security Solutions", was submitted on schedule in June 2023. 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 D1.4.
- As one of the relevant Work Packages, WP3 has contributed to the achievement of Milestone MS7 "Final implementation and deployment of the architecture", which was achieved on M33 through the submission of deliverables D3.3, D4.3 and D5.4. To this end, WP3 has implemented its security solutions and integrated them into the SIFIS-Home testbed and pilot, in concert with relevant partners contributing to WP5 and WP6, and by relying on the process for continuous integration and deployment of Software used in the project.
- The activities carried out within WP3 and their (intermediate) outcomes have been disseminated through international conference tutorials, seminars, lectures and other presentations, as well as through academic publications on international journals, conferences and workshops (as related to T7.1 in WP7).
- The activities carried out within WP3 and their (intermediate) outcomes have been duly taken as input to related standardization activities within the international body IETF (as related to T7.2 in WP7).

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)
In the reference period, the activity conducted in Task 4.1 followed three directions. First of all, further analytics have been studied, designed, implemented and they are now under testing. In particular, the **Face Recognition – Person Recognition** analytics has been designed and implemented as follows:

- Aim of the analytic: Person recognition is critical for identifying home resident users, guests, and intruders. Moreover, to provide smart personalized services to users based on their identities. Face recognition is done by training a model on resident users' images, and when a person enters the home or a room in the home, this person's face image is detected and compared to the trained model to classify the user based on the extracted features.
- Input Data: The face recognition analytic takes as input data the video frames produced by the surveillance cameras distributed into the controlled environment, such as the camera of the controlled device or the surveillance cameras deployed in the environment.
- Analytic Design: the privacy-preserving face recognition framework that has been developed uses Gaussian filters for image blurring or Autoencoders for image anonymization with different degrees of privacy (that could be determined using the approach describe in the following) to protect sensitive data. This model has been validated with a set of experiments on a well-known dataset, the Labelled Faces in the Wild (LFW) dataset. Figure 1 shows the entire workflow in a sample scenario, it starts with image capture and anonymization using Gaussian blurring on the user side. The resulting anonymized images are forwarded to the server to be processed for face recognition starting with a face detector OpenCV to detect all faces within an image. Detected faces are aligned and then converted to vectors. Finally, the faces are verified by comparing their representations with the representations of face images stored in the database. We use three deep learning models for face recognition: VGG-Face, Facenet512, and ArcFace.

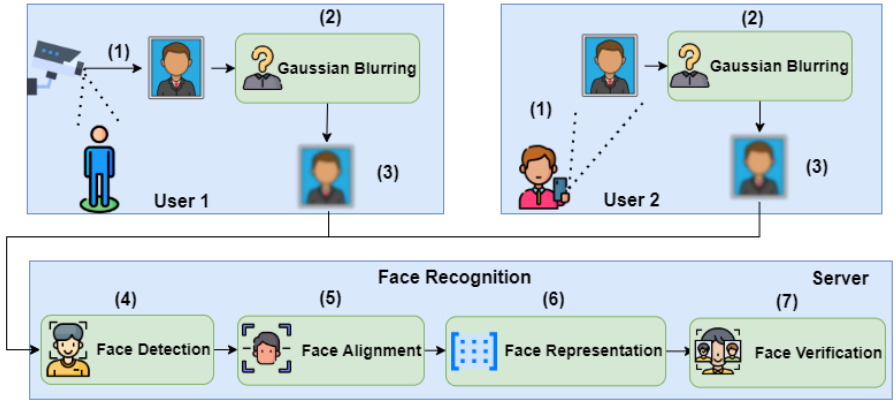


Figure 1: Privacy-Preserving Face Recognition Scenario

The SIFIS-Home face recognition analytic is composed by a pipeline of the following four components:

Face Detection: using the Haar Cascade classifier. Haar-like features are used to detect facial regions like eyes and nose, and they are determined using the integral image representation mechanism, and the AdaBoost

classifier is used to select only relevant Haar-like features that are known to improve the binary face classification algorithm results.

Face Alignment: face images might have several poses and expressions, which may affect the accuracy of the face detection and face verification models. Thus, to decouple these poses and expressions from the face identity and to reduce their effect on the face detection and classification algorithms, face alignment is used. For face alignment, we use a simple trigonometric method. This method detects eyes and eye coordinates as a first step and draws a triangle between eyes based on their centre locations. The angle of the lower eye needs to be computed, and this is done based on the horizontal line drawn between eye centres, computing the length of the three edges of the triangle between eyes using the Euclidean distance. Then, the angle is calculated with the cosine rule. Finally, the image is rotated based on this angle.

Face Representation: converts face images into vector embeddings, so that vectors of similar images for the same person are closer in distance among them. Trained Neural Networks (NN) for face recognition tasks do represent face images in the layer before the output layer. Therefore, these trained models on huge datasets can sufficiently represent new face images into high dimensional representations, and to extract and represent facial features of complex concepts.

Face Verification: compares face representations produced by the layer before the output layer of the NN used to perform face recognition. The output layer returns the classification of a face image compared to another one, whether they belong to the same person or not, based on semantic closeness. To measure semantic similarity, we use the cosine similarity metric, which finds the cosine of the angle between two representations.

Another analytics designed and developed in the reference period is the **Object Detection and Recognition one:**

- Aim of the analytics: This analytics concerns object recognition, where suspicious objects are identified within captured images or videos and their locations within the frame are determined. These suspicious objects can range from fire incidents to misplaced hazardous items like sharp tools. During the analysis phase, the system performs object recognition by identifying and classifying the objects in the images, along with their precise locations. If suspicious objects are detected, the user is promptly alerted, ensuring timely response and appropriate action. By integrating object recognition capabilities into the smart home system, it becomes capable of effectively identifying potential threats and alerting users to take necessary measures. This enhances the safety and security of the home environment by leveraging advanced image analysis techniques and automation.
- Input data: The object recognition algorithm takes as input the images or the video frames obtained from cameras positioned throughout the controlled environment.
- Analytics design: The analytics exploits the YOLOv3 model, and operates by dividing the input image into a grid, and predicting bounding boxes and class probabilities for each grid cell of such grid. The YOLOv3 model was trained on the COCO (Common Objects in Context) dataset which contains over 200,000 images from various contexts and 80 common object categories. The pipeline of the analytic is composed of the components shown in Figure 2.

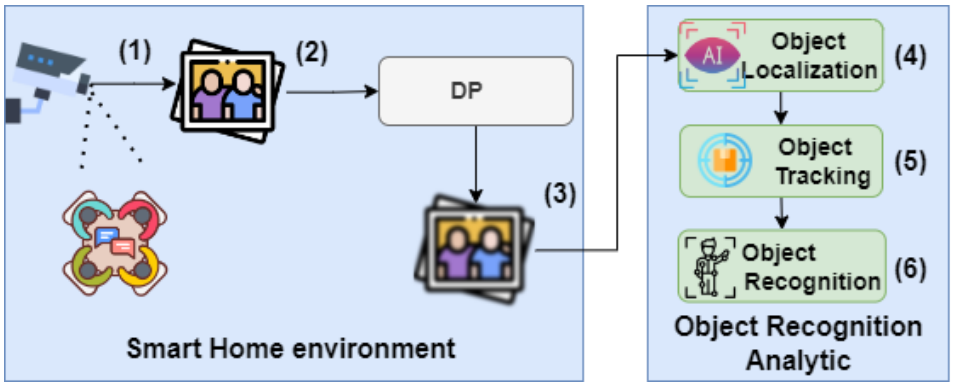


Figure 2: Privacy-Preserving Object Recognition Scenario

The analytics initially detects and localizes objects within the images or video frames and tracks them over time in the case of video streams. Finally, the detected objects are identified based on the COCO dataset objects that the YOLOv3 model was trained to recognize.

An additional analytics designed in Task 4.1 during the reference period is the **Multi-level Intrusion detection** one:

- Aim of the analytic: detecting intrusions attempt to a smart device exploiting and combining information collected at all levels of the smart home device stack. This would allow to detect and even prevent corruptions of smart home devices.
- Input data: the analytics gather the following data for each time period (called Time Frame): the system calls made by the device, the network data and the activities carried out by the device on the DHT. The primary features that describe the network flow are extracted from the network-level data using a features engineering process. The following table shows in more details some examples of the features that are taken into account for the previous categories.

Level	Feature	Feature description
kernel	switch	Context switch
	read	Read from a file description
	mprotect	Set protection on a portion of memory
	mmap	Maps files into memory
Network	pktl12	Packet size
	lat12	Time interval between two packets
	sflowpackets1	Number of packets in a subflow
DHT	GET	Number of GET operations performed on the DHT
	PUT	Number of PUT operations performed on the DHT

A number of machine learning techniques will be evaluated for the implementation of this analytics. We think that conventional machine learning classifiers could work well for our issue or at least we need to employ the simplest model which has consistent metrics. We should consider a vector of numerical features taken from the network flow, kernel, and DHT as Application level in only one time period. Each vector has a categorical label that distinguishes between benign and harmful behaviour. We have identified the cutting-edge machine learning classifiers that are appropriate for this classification challenge based on the data structure and the categorical problem to solve. The biggest model we have decided to try corresponds to Transformer Model, which it will be surely applied for application level.

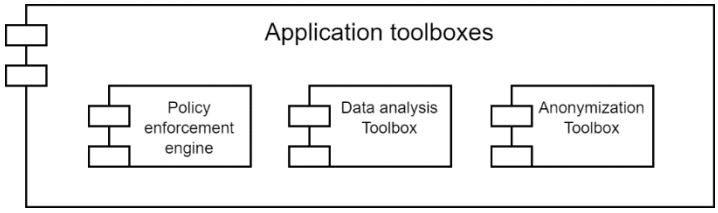
Classifier	**Advantages**	**Disadvantages**
Transformer	Attention technique	Big models
KNN	Few hyperparameters to tune	Slow computation in Real time
Decision Tree	Handles colinearity between features	No online learning
Random Forest	Tree Ensemble	No online learning
SVM	Handles outliers	Handles only independent features
AdaBoost	Ensemble model	No online learning

Furthermore, at the application level, a further analytics is being designed to identify the activity of the various applications installed on the device. This analytics would look for any signs of malicious activity, such as unauthorized access to sensitive data, or unusual activity that could indicate that a hacker is attempting to exploit a vulnerability in the application. The available works in this field focus on the detection and categorization of Android Malwares, still we are working to expand this kind of analysis to SIFIS-home device Applications. Briefly, a reverse-engineering tool for android platform is employed to get applications' API call graphs through which API call sequences are generated following Kahn Algorithm; this procedure is necessary in order to let sequences be consistent with the topology of the graphs. Finally, the Transformer model BERT is used for categorizing API call graph sequences, resulting in a classic NLP problem. The preliminary results we obtained on a dataset of Android malwares are really comforting, since we have reached 98% on malware detection and 93-94 % on malware categorization.

Besides the design and development of new analytics, the second direction followed in Task 4.1 concerns the integration of the analytics designed and developed in the previous period within the SIFIS-Home framework, in order to make them available to all the SIFIS-Home components. For instance, the System Protection Manager component of the Secure Lifecycle Manager subsystem could need to execute analytics on a dataset produced by a (set of) sensors (e.g., measuring the temperature or presence of people in a room). In particular, the Data Analysis Toolbox component has been designed and implemented to allow the execution of the analytics by the other components of the SIFIS-Home framework.

The Data Analysis Toolbox is the frontend of all analytics, interacts with the DHT to receive the requests to execute analytics from the other components of the SIFIS-Home framework, and manages the analytics execution invoking the specific analytics, getting back the results, and returning them to the requestor exploiting the DHT as well.

In order to enable their integration with the Data Analysis Toolbox, two services providing the analytics Faulty



Device Detection and Parental Control implementations have been implemented, and such services have been containerized using the docker technology. For each of these analytics a couple of DHT topics has been defined: one used by the SIFIS Home components to ask the SIFIS-Home framework (i.e., the Data Analysis Toolbox) to execute it, and the other used by the Data Analysis Toolbox to send back the result to the requesting component. For each topic a proper message format has been defined to represent the information needed for the analytics execution and for providing the results. The Data Analysis Toolbox has been configured in order to invoke the service corresponding to the topic published on the DHT.
The integration of analytics within the Data Analysis Toolbox component actually involved not only this Task, but also Task 4.2 and Task 4.4, i.e., also analytics from such tasks have been integrated within the SIFIS-Home framework following the approach we described above. However, for the sake of conciseness, the above description will not be repeated in the following.

The third activity carried out in Task 4.1 concerns data privacy protection, and involves the study of a novel approach for multi-party collaborative data analysis problems, where data utility (accuracy of the results and divergence between the original dataset and the anonymized dataset) is a requirement as well as privacy of shared data and explainability of the results. The proposed approach aims at trading-off data privacy, decision explainability (transparency), and data utility by analytically relating these three measures, evaluating how they impact each other, and proposing an optimization methodology to have the best possible trade-off among them. In particular, given a set of privacy and explainability requirements from the participants to a collaborative analysis problem, we propose a method to properly tune the parameters of the privacy-preserving mechanisms and explainability techniques to be adopted by all participants, obtaining the best trade-off among privacy, data utility and results explainability. This approach would be applied, for instance, in the case of analytics that are executed on the Cloud, which typically involve data coming from multiple smart homes equipped with the SIFIS-Home framework. As a matter of fact, in this case, the data are anonymized before being shared with the Cloud-based analytics by the Data Analysis Toolbox. However, smart home owners could have their specific (and possibly different) privacy (and also explainability) requirements concerning the data that are being shared. Hence, the proposed methodology can be used in the set-up phase of the SIFIS-Home environment for properly configuring the technique to preserve data privacy and the technique to provide explainability in order to obtain the best trade-off among privacy gain, data utility loss, and explainability. Another possible application of the above technique in the SIFIS-Home framework concerns the data that are shared by other applications running in the smart home. In this case as well, each of these applications could have its own privacy requirements concerning data sharing and once decided a common data anonymization technique, the approach could be exploited to choose the privacy degree that satisfies the application requirements and, at the same time, allows to reach a given accuracy of the results, still preserving a degree of explainability of the latter. This technique can

be applied to the analytics designed in Task 4.2 and Task 4.4 as well. However, for the sake of conciseness, the above description will not be repeated in the following.

Task T4.2: Network Intrusion Detection (M3-M33/CEN)
The input data consists of a network packet exchanged between the connected devices. The packets are captured, and relevant information parsed from them (port numbers, protocol identifiers, timestamps, IP addresses, etc...). Sensor values are collected from the IoT gateway in hex form.

For collecting all the network traffic between devices, the device running the IDS (intrusion detection system) must be connected to a mirror port or a network tap, or it must be a network gateway. If only the host traffic is monitored, then the device could be connected normally to the network.

The SPOT algorithm was tested by utilizing PCAPs (packet capture samples) of malware and Linux tools like Hping3 and Tcpreplay. Tcpreplay is used to modify and replay the malware packet captures and Hping3 is used to generate denial of service attacks.

SPOT algorithm needs the initial batch of observations to form thresholds for the monitored statistics. The thresholds are dynamic, and they adapt to a subtle change in the network by updating them based on chosen number of new observations. However, if the initial thresholds are triggered, the values over or under the threshold are not used to update the thresholds.

For the training and testing purposes, a network consisting of multiple sensors, IoT gateway, database/log server(virtual) and Linux workstation(virtual) was used for these tests. An implementation of SPOT called NetSpot was used to perform the initial tests, as it contains all the components and needed only to be built and configured on the machine which it was intended to be used on. NetSpot was run on a Raspberry Pi4, which was also acting as the IoT gateway for the sensors. NetSpot includes tuning parameters which can be used to tune it to meet specific needs.

For this test, SPOT was initialised by using 2000 observation from the normal traffic. After the thresholds were formed based on the observations, a denial-of-service attack was launched from the Linux workstation. As a results, the statistics that monitor the overall traffic over a certain time window and the ratio of tcp packets with a set synchronize flag were triggered and alarms were raised.

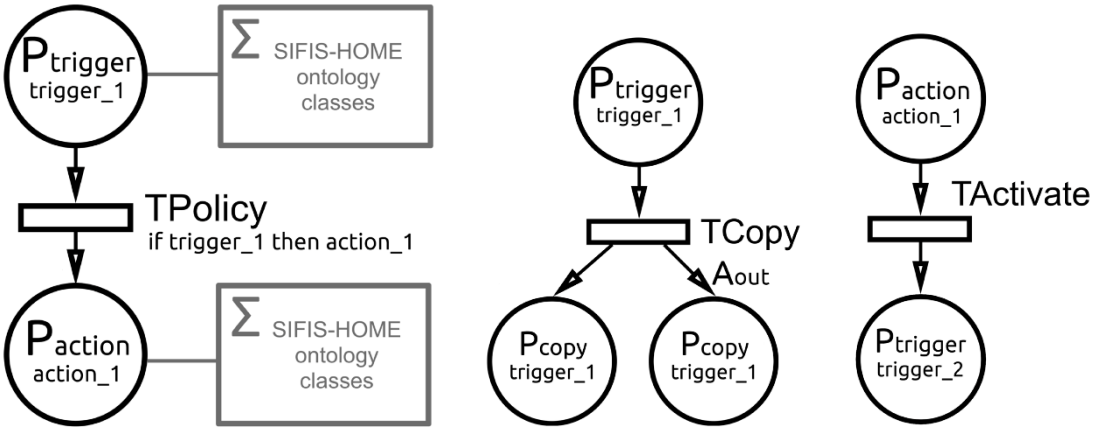
Netspot outputs: raw statistics, thresholds (SPOT will compute one threshold for each monitored statistic) and the alarms (in case of triggered threshold). Netspot can also send these to an influx database, a time series database for high write and query loads. The influxdata can then be visualized with Grafana. Alternatively, they can be saved locally on a file.

For the process of developing the IDS, further documenting has been made for privacy analysis and threat modelling the IDS solution. Privacy analysis documentation includes explanations of different qualities of this IDS from a privacy point of view. The threat model of the system explains about the potential security issues and mitigations when it is integrated to SIFIS-Home.

Integration measures of the IDS to SIFIS-Home solutions have also been started. This includes the start of developing a control solution "NetSpotControl" service for the system. The solution is planned to run as a docker container where the controlling program provides HTTP REST API for other services. The controlling service is designed to run netspot programs and collect data to the database.

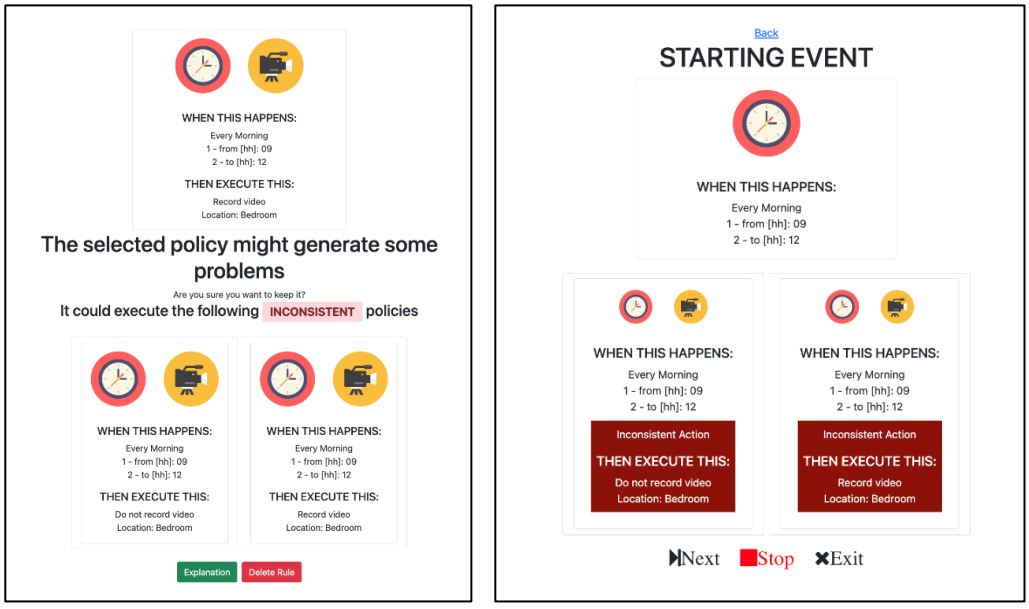
Task T4.3: Analytics for policy enforcement (M3-M33/POL)
The first months (M19-M24) have been dedicated to the refinement of the preliminary implementation of the Policy Enforcement Point (PTP), i.e., the module that is responsible for translating and checking high-level security policies such as “Do not record sound in the living room tonight.” We focused on simplifying and fine-tuning the code to optimize performances in the translation task. In parallel, the *sifis-home ontology* has been extended and integrated with additional devices and applications to support a larger set of policies. Furthermore,

we refined and explored variations in the novel model based on Semantic Web technologies and Petri Networks – inspired by a state-of-the-art Semantic Colored Petri Networks approach – that is used by the PTP module to capture potential inconsistencies and redundancies among high-level security policies at run time.



Petri nets are bipartite directed graphs in which directed arcs connect places and transitions. Places may hold tokens, which are used to study the dynamic behaviour of the net through transitions. As shown in the figures above, in our case places may represent "triggers" of a policy (e.g., "tonight in the living room") and "actions" of a policy (e.g., "do not record sound"). Actions of a policy may activate triggers of other policies ("TActivate" transition), while the net duplicates places related to policies with the same trigger ("TCopy" transition). Furthermore, places are labelled with the corresponding OWL classes extracted from the *sifis-home ontology*. By firing a transition at a time, tokens move in the net by giving the idea of a possible execution flow, and the associated semantic colours can be used to discriminate between possible inconsistencies and redundancies. At the end of the period M19-M24, we also managed to describe the approach in a research paper presented at the 5th International Workshop on Emerging Technologies for Authorization and Authentication (ETAA 2022), held in Copenhagen (Denmark).

During months M25-M26, we instead focused more on the graphical user interface of the PTP module through which end users can define and check high-level security policies to be introduced in the SIFIS-Home ecosystem. To this end, we internally conducted a heuristic evaluation and different usability studies to improve the design of the PTP's UI. Besides usability, special attention was also posed to the accessibility of the interface. The design activities have been mainly focused on the "step-by-step" execution tool, through which users can visually simulate the execution of their policies.



Results of the redesign of the PTP's module are shown in the figures above and have been presented together with the Semantic Petri Net approach at the 5th International Workshop on Emerging Technologies for Authorization and Authentication (ETAA 2022), held in Copenhagen (Denmark). We are currently planning further research studies to compare the adopted definition paradigm with alternative strategies, e.g., to explore the effectiveness of using solutions exploiting a "jigsaw metaphor" through which triggers and actions of a security policy are represented by puzzle pieces that can be connected together.

The remaining months have been mainly dedicated to the definition and documentation of the APIs exposed by the PTP module and to the integration of the PTP module in the SIFIS-Home framework. To this end, the PTP module has been containerized using Docker technology.

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

- the refinement of the preliminary implementation of the PTP module;
- the extension of the sifis-home ontology;
- the refinement of the novel Semantic Colored Petri Net approach;
- a redesign of the PTP's UI, with a particular focus on the accessibility aspect;
- the development of a documentation for the APIs exposed by the PTP module;
- the containerization of the PTP module using Docker.

Task T4.4: Privacy Aware Speech Recognition and Smart Service Analytics (M3-M33/CNR)
In the reference period the activity conducted in Task 4.4 focused on speaker verification and identification through voice analysis, as described in the following.

Speaker verification through voice analysis

- Aim of the analytic: The speaker verification is the process of authentication of a person exploiting the human biometric voice aspect. The use of this aspect can guarantee unobtrusiveness to the authentication mechanism ensuring a good level of security. Such service is exploited by the SIFIS-Home system to verify the identity of the person who is intended to use a protected smart-device.
- Input Data: The speaker verification analytic takes as input data audio streams or files recorded by users.
- Analytic Design: A privacy-preserving model has been developed based on Biometric Information Protection with Cryptography and Identity Hashing. We compose a speaker verification mechanism that utilizes the ECAPA-TDNN model. Figure 3 shows the entire workflow in a sample scenario, it starts with audio recording and encryption on the user side. The resulting encrypted audio files are either processed locally or forwarded to the server to be processed, starting with audio file decryption to get the original content, and then processed to obtain speaker embedding for each person's identity that is being verified. Then, a computation of the cosine similarity between the two embeddings is performed, and the speaker verification model is used to predict whether the two audio files belong to the same user identity or not. Next, the predicted results might be used to perform an action on the server side or to be encrypted and shared with the user who requested the speaker verification service.

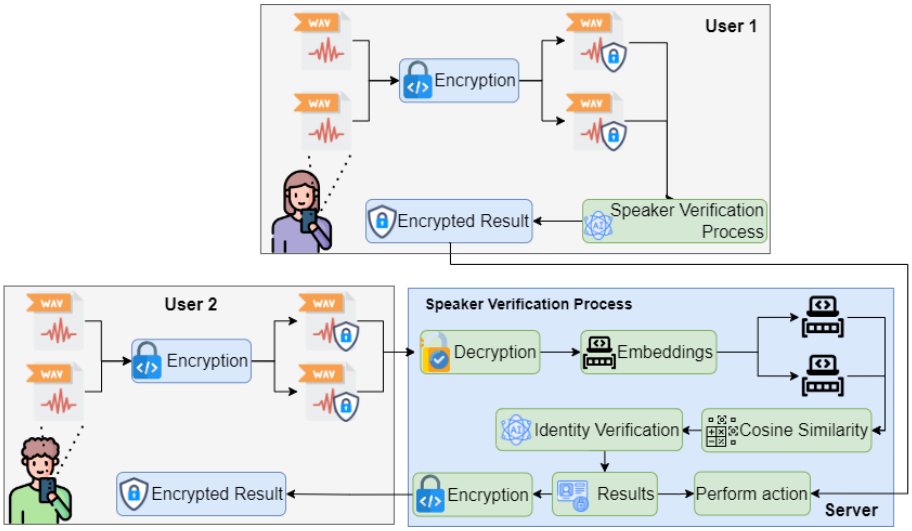


Figure 3: Privacy-Preserving Speaker Verification Scenario

The architecture of the ECAPA-TDNN model is shown in Figure 4. ECAPA-TDNN model employs ECAPA Time Delay Neural Networks (TDNNs) derived embeddings, that classifies inputs as a binary prediction of yes or no verification results.

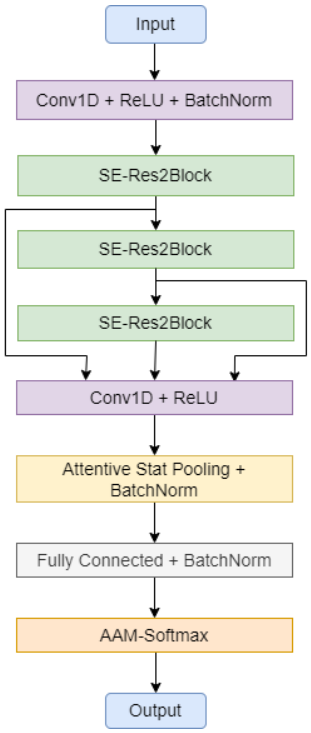


Figure 4: ECAPA-TDNN Model for Speaker verification

Speaker identification through voice analysis

- Aim of the analytic: Speaker recognition is the identification of a person from the characteristics of their voice. In the SIFIS-Home environment, it is fundamental to understand the identity of a person in order to grant the right privileges according to the policies set for that person. The speaker recognition system will run in the background to understand the identity of the persons present in the environment and it will communicate them to the smart-home control manager which will grant the execution of some actions based on the policies set, e.g., the use of a smart device will be possible only if a set of persons are identified in the environment.
- Input Data: The speaker identification analytic takes as input data audio streams or files recorded by users.

- Analytic Design: Like the speaker verification model, ECAPA-TDNN model has been used for speaker identification, but this model identifies the speaker among several identities instead of comparing two audio streams only. The Speaker identification model can utilize Biometric Information Protection with Cryptography and Identity Hashing for privacy protection. The model starts with audio recording and encryption on the user side. The resulting encrypted audio files are either processed locally or forwarded to the server to be processed, starting with audio file decryption to get the original content, and then processed to obtain speaker embedding for each person's identity that is being verified. Then, a computation of the cosine similarity between the two embeddings is performed, and the speaker verification model is used to predict whether the two audio files belong to the same user identity or not.

Besides the design and development of the above-mentioned new analytics, in Task 4.4 we also developed a novel version of the **Speech Recognition** analytics with the aim of providing results with a high degree of accuracy. In particular, we implemented a further machine learning model for the speech recognition task in addition to the Mozilla DeepSpeech model based one we developed in the previous period. Developed by Open AI and released in 2022, the new model, called Whisper, is a sequence-to-sequence model that has been trained on a large variety of data from multiple languages. Trained on 680,000 hours of multilingual data collected from the web. Never before has this amount of data been used for supervised training. Thus, Whisper achieves higher accuracy than Mozilla's DeepSpeech model with a much lower word error rate to ensure the performance of our machine learning model.

Anomaly Detection in Audio Signals

- Aim of the analytics: Performing audio anomaly detection in smart homes enhances the overall safety and security of the occupants by identifying unusual or potentially dangerous events that may occur within the home environment from the noise they produce. This includes detecting anomalies such as breaking glass, loud and sudden noises, unusual patterns of speech or conversation, or other signs of potential threats or emergencies. By continuously monitoring audio signals in the smart home, the system can quickly identify and raise an alert for any abnormal activities.
- Input data: The input data for audio anomaly detection in smart homes is the audio signals captured within the smart home environment, captures using microphones or audio sensors deployed in the smart home.
- Analytics Design: the analytics exploits the IBM MAX audio classification model, which is a multi-attention classifier designed to analyze and categorize audio data into various predefined classes or labels. The classifier leverages the power of deep neural networks to learn patterns and features from large-labeled audio datasets, allowing it to make predictions on new, unseen audio inputs. The core component of the audio classifier is a deep neural network model consisting of multiple layers, such as convolutional layers, pooling, and fully connected layers. These layers are designed to learn hierarchical representations and capture relevant audio features for classification. The model is designed to support 527 classes, defined within the Audioset Ontology, and provides as result the top 5 classes the noise could belong to, along with the corresponding probabilities.

Contribution per partner to WP4

Partner	Contribution
CNR	Led WP4 activities. Designed and implemented the Data Analysis Toolbox, which manages all the analytics developed in WP4, and integrated it with the analytics developed in the previous period. Designed and developed new analytics in Tasks 4.1.and T4.4. Organized bi-weekly meetings to coordinate and follow the design and development of new analytics, as well as to enable the integration of the analytics designed and developed in the previous period within the SIFIS-Home framework through the Data Analysis Toolbox.
FSEC	Regular participation to WP4 meetings concerning the development, integration, privacy assessment, and threat modelling of analytics created within WP4. Developing the Network Anomaly Detection analytic in particular.
DOMO	Followed the WP4 activities. Dedicated meetings with WP4 partners to show the usage of the DHT Manager component and its REST and WebSocket APIs. Prepared a number of example applications in Python language showing the usage of the DHT WebSocket API.

	Dedicated meetings with CNR focused on the Node Manager component design. Provided support to all the WP4 partner for integrating the WP4 components in the project pilot.
RIO	Participation to WP4 meetings, planning and improvements to analytics services, particularly Data Flow Analytic.
SEN	Regular participation to WP4 meetings concerning the overall development and integration, of different analytics as well as development of SEN own anomaly detection analytics.
RISE	Followed the WP4 activities.
CEN	Developing Network based Intrusion Detection System
POL	The leader of task T4.3 “Analytics for policy enforcement” provided regular participation to WP4 meetings and focused its contribution on the Policy Enforcement Point (PTP).

Achievements

During the reporting period, the following have been achieved:

- Design and development of new analytics;
- Improvement of the performance of the Speech Recognition analytics through the adoption of a more recent model, the Whisper one;
- Design and development of the Data Analysis Toolbox, which is the component that interfaces the analytics with the DHT. Thid enables the other components of the framework to invoke the analytics developed in WP4 just by publishing a message with the topic corresponding to such analytics on the DHT. The Data Analysis Toolbox is modular; thus, it will be straightforward to extend it to allow the integration of further analytics;
- Integration of most of the analytics developed in the previous period within the Data Analysis Toolbox, hence making them available to the rest of the SIFIS-Home framework;
- Definition of a novel approach, to be adopted when multiple parties collaboratively exploit the same analytics service (e.g., when a set of smart homes set up a common analytics service) to properly tune the parameters of the adopted privacy-preserving mechanisms (i.e., the privacy degree), and to take also into account the usage explainability techniques, in order to obtain the best trade-off among privacy, data utility and results explainability;
- Refinement of the novel model based on Semantic Web technologies and Petri Networks to capture potential inconsistencies and redundancies among high-level security policies at run time;
- Redesign of the graphical user interface for the PTP module, achieved through a heuristic evaluation and several usability tests, with a particular focus on the "step-by-step" execution tool - i.e., a tool through which users can visually simulate the execution of their high-level security policies.

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)
D5.1 delivered in the end of May 2022 define the preliminary version of the test bed and since then we have continued working on the test bed and come to an agreement with all partners of exactly how the test bed should look like and who is responsible for what part. The test bed has been live since January 2022 and new components are continuously deployed once the development is ready. Several components have also been updated during the period.

Task T5.2: Component Implementation, Integration and Deployment (M12-M33/SEN)
D5.2 was delivered in September 2022 and describes the status of Task 5.2 at that point in time. After D5.2 some integration components have been added to solve technical difficulties. Further, we now have agreed upon a responsible partner to develop every component in the architecture while we previously had some components without owner. The work in the task is now focusing on driving the development and integration progress.

Task T5.3: Evaluation and Validation (M20-M33/LUM)
As the new code contributions are landing to the Github organisation code review and feedback is being provided. Integration tests are being planned but not yet performed since the components aren't fully integrated yet.

Contribution per partner to WP5

Partner	Contribution
CNR	CNR has regularly participated to all WP5 meetings acting as coordinator of the interaction between the WP1 results and the WP5 integration. Moreover, CNR has provided the infrastructure for the simulated testbed and took care of the deployment infrastructure.
ERI	Regular participation to the WP5 meetings.
FSEC	Regular participation to WP5 meetings concerning the deployment and integration of components in the SIFIS-Home testbed. Contribution to D5.2 on behalf of FSEC's components.
LUM	Regular participation to the WP5 design meetings and contributed to the design of the SIFIS-HOME testbed. Started the development of simulated WoT devices and started reviewing the code contributions that are now landing the Github organisation.
DOMO	Regular participation to the WP5 design meetings and contributed to the design of the SIFIS-HOME emulated testbed. Design and development of the DHT Manager component. Design and development of the Fiware API component. Preparation of Ansible scripts for deploying the SIFIS-HOME component in the emulated testbed in an automated way. Co-authored deliverable D5.2, D5.3, D 5.4.

RIO	Participation to WP5 meetings. Took responsibility and started the implementation of the SIFIS-HOME mobile application development. Integration of simulated devices from WP6 to be run with Docker on Panarea server.
SEN	Sensative is leading WP5 and is also actively contributing how to apply the WP1 architecture practically to implement the test beds. Sensative is also implementing large parts of the SIFIS Home UX like the Device Manager, Installation manager, Home and Alarm/logs and as well as implementing the FIWARE Context Broker RATATOSK used in SIFIS Home. During the period the focus, except leading WP5, has been on driving the development progress of the SEN owned components.
RISE	Regular participation to the WP5 design and integration meetings; integration of security solutions from WP3 into the SIFIS-Home testbed, supported by internal technical workshops in order to plan, assist, monitor and execute the integration activities; co-authored deliverable D5.2; co-authored and reviewed deliverable D5.4; regular maintenance and update of a single, organic codebase comprising the implementation of the security solutions from WP3.
CEN	Integrated IDS into framework. Work completed
POL	Followed the WP5 activities and contributed to the integration of the Policy Enforcement Point (PTP) developed in WP4.

Achievements

During the reporting period, the following have been achieved:

- First version of SIFIS-Home testbed submitted (D5.1);
- First version of SIFIS-Home Security Architecture Implementation submitted (D5.2).
- Final version of SIFIS-Home testbed submitted (D5.3).
- Final version of the SIFIS-Home Security Architecture Implementation submitted (D5.4)

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/DOMO)
WP6 started its activities by defining a set of smart home use cases that we demonstrated and tested through the development of a physical testbed employing the SIFIS-HOME framework. For every use case we reported the functional, non-functional and security requirements. All the details of the defined use cases and the devices that we used for the testbed can be found in D6.1 and D6.3.

Task T6.2: Use Case Security and Privacy Goal Refinement (M15-M30/RIOTS)
During the reporting period, this task involved definition of the requirements concerning security and privacy aspects of the smart use case. Additionally, the acceptance tests were defined for each requirement. As D6.1 and D6.2 are demo deliverables, we accepted a flexible approach to both security and privacy aspects for the system demos. The work has been done in parallel of the implementation and the requirements are to be verified before the end of project. A special focus has been made on data privacy, system resiliency, safety access privileges to the physical resources, configuration interfaces and specific services and applications. Riots has had several points of special interest: privacy in regard to energy savings; privacy in regard to sharing economy (data tied to the individual vs. data tied to the smart home apartment); how to balance (data) security with the responsibility and power resulting from collecting and controlling big data.

Task T6.3: Use Case Design and Implementation (M20-M34/DOMO)
This task has been devoted to the development of a physical testbed employing the SIFIS-HOME framework through which we demonstrated and tested the use cases presented in D6.1 and D6.3. Our testbed is composed of both Smart Devices and Not so Smart Devices. We considered the DoMO Gateways and standard amd64 Laptops as smart devices and the DoMO WiFi actuators as not so smart devices. The following activities related to this task have been carried out:

1) Web of Things compliant firmware implementation for the DoMO WiFi actuators,
2) DHT Manager and NSSD Manager implementation,
3) development of a SIFIS-HOME OpenWrt distribution for the DoMO Gateways,
4) production of dedicated Docker Images for every SIFIS-HOME component,
5) production of the docker-compose files to be used in the pilot,
6) integration of the different SIFIS-HOME components in the pilot,
7) development of the SIFIS-HOME Mobile Application and the Fiware API component,
8) development of the domo-scheduler, domo-bootstrap, light-manager, SIFIS-SD-nginx-serverm,
9) VPN configuration. Additional details of the final pilot implementation are reported in deliverable D6.4.

Task T6.4: Experimental Evaluation and Validation (M20-M36/LUM)
As per task T5.3 the main activity so far had been reviewing the other partners code contribution while the integration of the components is still pending.

Contribution per partner to WP6

Partner	Contribution
CNR	CNR has participated to the WP6 design meetings.
ERI	Regular participation to the WP6 design meetings.
FSEC	Regular participation to the WP6 design meetings to better link WP1 and T4.2 topics with the pilot.

LUM	Provide support regarding the integration of Rust within OpenWrt and review the code contributions from the other partners as it lands. Help debugging OpenWrt-specific issues regarding packaging and bring up the system on the target hardware.
DOMO	Leadership of WP6 and Task 61 and 6.3. Design and implementation of the DHT Manager component, NSSD Manager Component, Fiware API component, domo-scheduler component, domo-bootstrap, SIFIS Light Manager, SIFIS-SD nginx server, VPN Manager solution. Development of a Web of Things compliant firmware for the DoMO WiFi actuators. Preparation of a SIFIS-HOME OpenWrt distribution for the DoMO gateways. Responsible for the integration of all the SIFIS-HOME components in the WP6 pilot. Performed the validation of the different smart home use cases employing the WP6 testbed. . Author of D6.2, D6.3 and D6.4.
RIO	Participation to the WP6 design meetings. Leader of Task 6.2. Integration of Riots devices to SIFIS-HOME architecture as part of WP6.
SEN	WP5 and WP6 is based on the same code base. SEN is developing components that will be used in both WP5 and WP6. Further SEN has joined and participated in WP6 design and implementation meetings.
RISE	Regular participation to the WP6 design and integration meetings; provided feedback on security aspects concerning workflows in the pilot use case; integration of security solutions from WP3 into the SIFIS-Home pilot, supported by internal technical workshops in order to plan, assist, monitor and execute the integration activities.
CEN	Developed Smart Device Mobile API
POL	Regular participation to the WP6 design meetings, provided aspect on the definition of the use cases definition.

Achievements

During the reporting period, the following have been achieved:

- Definition and validation of 19 different smart home use cases that we demonstrated and tested successfully through the usage of a physical testbed employing the SIFIS-HOME framework.
- Integration and testing of the SIFIS-HOME components in a smart home pilot involving commercial physical devices.
- WoT firmware implementation for the DoMO WiFi actuators: we implemented a WoT compliant firmware for the DoMO WiFi actuators. The firmware has been developed using the C++ language and the PlatformIO framework.
- OpenWrt distribution for the DoMO gateways: we prepared a specific OpenWrt distribution for the DoMO gateway that includes the SIFIS-HOME software components to be used. DHT Manager implementation: The SIFIS-HOME DHT is a component that offers a completely distributed publish/subscribe mechanism through which SIFIS-HOME applications can exchange messages. It has been developed using the Rust language.
- NSSD Manager implementation: The SIFIS-HOME NSSD Manager is the SIFIS-HOME component responsible for interacting with the NSSD devices present in the house. It has been developed using the Rust language. Docker images: we prepared specific GitHub actions that allow building the different SIFIS-HOME components for both arm64 and amd64 architectures. We also prepared a dedicated Docker Image for every SIFIS-HOME component that has been used and integrated in the WP6 pilot.
- Docker-compose files: we prepared a docker-compose file that is used on both the DoMO gateways and the pilot Laptops. The docker-compose file contains the list as well as the configuration of all the SIFIS-HOME services that should be executed on a SD.
- VPN server and VPN manager implementation: we developed a technical solution that uses i) a VPN server, ii) a VPN client and iii) a nginx proxy server, that makes services running on the SDs accessible from a remote side. In detail, it makes the DHT Manager web service, the privacy dashboard panel and the policy translation point panel running on a SD deployed in the house available from a remote side.
- Fiware API component implementation: this component forwards the persistent messages published through the DHT to the Ratatosk FIWARE Context broker that is part of the Yggio instance residing on the SIFIS-Home cloud. Also, it forwards commands entered by the user in the Yggio user interface to the DHT.

- Mobile application implementation: the Mobile Application allows users to easily manage the SIFIS-Home network basic functionalities. This includes listing the installed devices within the home, enabling users to perform various actions on these devices, such as collecting environment measure readings, or controlling actuators, or turning devices on or off. Additionally, the Mobile Application provides access to system logs for monitoring purposes, as well as the ability to install third-party applications directly into the SIFIS-Home framework, in order to extend the capabilities of the system. The Mobile Application was written in Javascript and Vue utilizing the NativeScript framework and the Stackblitz development environment.
- domo-bootstrap implementation: we developed a Web server application, that runs on the DoMO gateways composing the pilot, that offers an API through which it is possible to initialize new Smart Devices. In particular, the application allows a Smart Device to receive all the information it needs to join a SIFIS-HOME network.
- domo-scheduler implementation: the role of the domo-scheduler is to elect one leader device among all the different SDs that are present in a certain SIFIS-HOME network, in a dynamic way. The leader device is the only one allowed to execute specific services of the smart home, that are named cluster services.
- SIFIS-SD-nginx-server implementation: it is a nginx proxy server that is used to protect the web services running on the SDs from external access.
- SIFIS Light Manager implementation: such component takes care to turn on and off the physical lights of a certain room when the physical buttons of the room are pressed/released by the users of the smart home.

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)

From month 18 to month 36, the dissemination task has been extremely active. The partners of SIFIS-Home have organized 2 international scientific workshops as satellite events of the NetSoft and ESORICS conference and have presented 4 papers in international conferences and workshops, including the mentioned ones. To reach the

general audience, the coordinator participated to a round table at NEXA centre in Turin, to raise awareness about the problematics addressed by the SIFIS-Home project and discuss how SIFIS-Home can effectively tackle such problematics. In January 2023, a Spotify podcast in Italian has been released by CNR discussing on the cyberphysical systems security and briefly presenting the SIFIS-Home project. At the end of January 2023 a joint press-release has been published together with 7 other projects funded under the same call of SIFIS-Home. Finally, SIFIS-Home participated as exhibitor to the IoT Solutions World Congress and Cybersecurity Congress in Barcelona, an event counting more than 15k attendants, 1 interview was given during the event for the press present at the event. Demonstrations presented during the event.

A Webinar including representatives of three of the projects that participated in the Cybersecurity Congress, including SIFIS-Home, has been organized by CEN. The webinar featured an invited speaker from the EU parliament and a panel with coordinators and members of the three involved projects. All activities have been reported and advertised through our website. Also, all events organized by SIFIS-Home are available on our YouTube channel.

Task T7.2: Standardization (M1-M36/RISE)
Within this task, and building on their long-term experience and track record, 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].
- Static Context Header Compression (SCHC) [7.2-SCHC].

The standardization proposals are documented as technical specifications in the form of Internet Drafts, and have been developed by taking as input most of the activities from WP3 "Network and System Security".

At the time of writing, these amount to a total of 23 documents, of which: 1 has been published as a Proposed Standard RFC; 1 has been approved for publication as a Proposed Standard RFC; publication has been requested for 4 of them, as Proposed Standard RFCs; 9 more are adopted by a Working Group; 8 are individual submissions.

The full list of IETF Internet Drafts and published standards is available in the project website at [7.2-LIST].

The following highlights pertain to the period covered in this technical report.

- In August 2022, the OSCORE profile of the ACE framework has been published as RFC 9203 (Proposed Standard) [7.2-DOC1].
- In November 2022, the specification of the EDHOC and OSCORE profile of ACE has been adopted as an ACE Working Group document [7.2-DOC2].
- In December 2022, publication has been requested by the LAKE Working Group for the specification of the EDHOC key establishment protocol [7.2-DOC3], as Proposed Standard.
- In March 2023, publication has been requested by the ACE Working Group for the specification on key management for OSCORE groups using the ACE framework [7.2-DOC4], as Proposed Standard.
- In June 2023, publication has been requested by the ACE Working Group for the specification on the notification of revoked access tokens in the ACE framework [7.2-DOC5], as Proposed Standard.
- In August 2023, publication has been requested by the CoRE Working Group for the specification on using EDHOC with CoAP and OSCORE [7.2-DOC6], as Proposed Standard.
- In August 2023, publication has been approved for the specification of the EDHOC key establishment protocol [7.2-DOC3], as Proposed Standard.
- Continued the work on the co-authored, active 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.

- Participation to the Hackathons and Meetings IETF 114 (Philadelphia, USA, July 2022), IETF 115 (London, UK, November 2022), IETF 116 (Yokohama, Japan, March 2023) and IETF 117 (San Francisco, USA, July 2023).
- Participation to regular Working Group virtual interim meetings and in official interoperability events aimed at testing implementations of standard proposals.

In addition, Luminem has been involved in the World Wide Web Consortium (W3C) [7.2-W3C] and specifically in the W3C Web of Things (WoT) Community [7.2-WOT], where it is now a full-fledged member and has been active within the WoT Interest Group, Community Group and Working Group [7.2-WOT-WG].

The contribution in W3C WoT is related to the activities carried out in WP2, and concerns the overhaul of the Thing Description 2.0 information model, in particular regarding the WoT-Profile and the Protocol Bindings Templates to address the concerns on describability, ultimately to ensure semantics interoperability of the used information models. Furthermore, Luminem contributed with a from-scratch Rust implementation of WoT standards, also integrating the SIFIS-Home Risk/Hazard labels in simulated things.

The following compiles a list of highlights and selected activities of Luminem in W3C, and especially in the different Task Forces of the WoT Working Group.

- A new, from-scratch Rust implementation of WoT standards, covering:
  - Thing Descriptions & Binding; profiles for Servients; Discovery
  - Demo-things, integrating the SIFIS-Home Risk/Hazard labels in simulated Things
- Pushed activities on Profiles towards support for constrained consumers.
- Contribution to a second implementation of the Served Side Event HTTP Profile.
- Addressed issues of the Things Description standard.
- Provided several feedback on other implementations and interoperability sessions.
- Authored a use-case document, based on the SIFIS-Home Risk/Hazard labelling:
  - https://github.com/w3c/wot-usecases/blob/main/USE-CASES/hazard-annotations.md
- Presented the Rust implementation at RustLab 2022 (Florence) and the WoT CF Meeting.
- Presentation of related relevant topics at TPAC 2023 WoT, in a joint session with the "JSON for Linking Data" Community Group and the "RDF Dataset Canonicalization and Hash" Working Group. Topics include:
  - Degraded consumption of Thing Description
  - JSON-LD restrictions in the current Things Description

Building on the above, further contributions are also planned, as to the alternative serialization panel on YAML-LD and CBOR-LD, which, with some limitations, are already supported by WoT Thing Description.

[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-SCHC] https://datatracker.ietf.org/wg/schc/about/
[7.2-LIST] https://www.sifis-home.eu/index.php/standardization/
[7.2-DOC1] https://datatracker.ietf.org/doc/html/rfc9203
[7.2-DOC2] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/
[7.2-DOC3] https://datatracker.ietf.org/doc/draft-ietf-lake-edhoc/
[7.2-DOC4] https://datatracker.ietf.org/doc/draft-ietf-ace-key-groupcomm-oscore/
[7.2-DOC5] https://datatracker.ietf.org/doc/draft-ietf-ace-revoked-token-notification/
[7.2-DOC6] https://datatracker.ietf.org/doc/draft-ietf-core-oscore-edhoc/
[7.2-W3C] https://www.w3.org/
[7.2-WOT] https://www.w3.org/WoT/
[7.2-WOT-WG] https://www.w3.org/WoT/wg/

Task T7.3: Business Planning and Commercial Exploitation (M7-M36/FSEC)
During the reporting period, this task has focused on finalizing D7.6 Final Business and Commercial Exploitation plan, including the analysis of Key Expoitable Results (KERs) of the project and their exploitation and impact potential, as well as a specific business and exploitation plan for the main result of the project, the SIFIS-Home Framework, including sustainability and monetizing plans. Furthermore, partners have updated and elaborated their individual exploitation plans to ensure effective exploitation of the solutions developed in the project. Further details of this work is reported in the D7.

The consortium also participated in a joint dissemination and exploitation event with other 4 projects funded by the same call in the IoT Solutions World Congress and Cybersecurity Congress held jointly in Barcelona 31.1.-2.2.2023. The event served as a key dissemination and exploitation activity for the project, as the SIFIS-Home project showcased preliminary results and demonstrations at a shared exhibition booth and stand with daily presentations. The activity offered an opportunity to receive feedback from potential end users and customers. The project partners also published a joint press release about the event. In addition, especially the industrial partners have participated in 23 industrial events to showcase the project to potential end users and customers within the target markets. Further details of the events are described in the section 2.3 of this document. The full list of planned and participated exploitation events, which have been selected according to their relevance and impact to the project topic and developed solutions, are also reported in D7.6 report.

Figure. SIFIS-Home project poster material for the joint exhibition at the IoT Solutions World Congress & Cybersecurity Congress 31.1.-2.2.2023 in Barcelona.

Contribution per partner to WP7

Partner	Contribution
CNR	Organization of the SECSOFT and ETAA workshops, production of scientific papers, participation to dissemination events in Italy for presenting the SIFIS-Home project activities and mission.
ERI	Publication of papers in international journals; presentation at international conference tutorial; driving in IETF security standardization; authorship of Internet Drafts and RFCs; participation in Working Groups and related activities.
FSEC	Management and coordination of the WP7 and T7.3 activities. Organization of WP7 monthly meetings and dedicated sessions for T7.3 work. Coordination of the project participation to the joint dissemination and exploitation event in IoT Solutions World Congress and Cybersecurity Congress in Barcelona 31.1.2023-2.2.2023. Contributions to T7.1 with dissemination and communication activities, especially creating content via the social media, project website and participation to industrial events. Editor and main author responsibility of D7.6 and internal reviewer of D7.5.
LUM	Help with the organization of the WoT Community Meetups, presented SIFIS and wot-rust at the rustlab.it 2022 and the first WoT Community online Meetup. Contributed external feedback to the WoT Thing Description, Profile and Binding Templates as implementor.
DOMO	Regular participation to the WP7 meetings.
RIO	Regular participation to the WP7 meetings. Business model development in cooperation with FSEC.
SEN	Sensative has participated in the WP7 regular meeting and performed all related tasks assigned to SEN. SEN will join the IoT solution world congress in Barcelona 31.1.2023 to 2.2. 2023 and support the dissemination of SIFIS Home. During the reporting period SEN also released all the components developed in SIFIS Home as open source as well as released them commercially on top of Sensative's horizontal IoT integration platform Yggio.
RISE	Enforced leadership of Task T7.2; papers published in international workshops, conferences and journals; presenter at international conference tutorials, seminars and lectures; strong regular engagement in IETF standardization, including leadership of one Working Group, authorship of several Internet Drafts, and key participation to meetings and other related events; co-authorship and main responsibility of deliverable D7.5; reviewed deliverable D7.6.
CEN	Social media channel updates. Publication of papers in international journals. Organized SecTALK seminar event for academia and private sector.
POL	Publication of papers in international journals. Organization of the "156° Mercoledì di Nexa" a round table discussion, with dissemination purpose toward the general audience, which has been entirely focused on the presentation of the SIFIS-Home project, reporting the relevance of the addressed topics. The event has been followed mainly via webstream and it is currently available on the NEXA YouTube channel. The discussion is in Italian.

Achievements

During the reporting period, the following have been achieved:

- 2 academic workshops organized and participated with a presentation (ETAA 2022 and SECSOFT 2022).
- 5 seminars organized and participated, including academic and industrial audience.
- 4 published journal articles; 5 published conference papers.
- In August 2022, the OSCORE profile of the ACE framework has been published as RFC 9203 (Proposed Standard) [7.2-DOC1].
- In November 2022, the EDHOC and OSCORE profile of ACE has been adopted as an ACE Working Group document [7.2-DOC2].
- In December 2022, publication has been requested by the LAKE Working Group for the EDHOC key establishment protocol as Proposed Standard [7.2-DOC3].
- In March 2023, publication has been requested by the ACE Working Group for the specification on key management for OSCORE groups using the ACE framework [7.2-DOC4], as Proposed Standard.

- In June 2023, publication has been requested by the ACE Working Group for the specification on the notification of revoked access tokens in the ACE framework [7.2-DOC5], as Proposed Standard.
- In August 2023, publication has been requested by the CoRE Working Group for the specification on using EDHOC with CoAP and OSCORE [7.2-DOC6], as Proposed Standard.
- In August 2023, publication has been approved for the specification of the EDHOC key establishment protocol [7.2-DOC3], as Proposed Standard.
- Standardization contributions of Luminem in the World Wide Web Consortium (W3C), as a new full-fledged member involved in the W3C Web of Things (WoT) Community within the WoT Interest Group, Community Group and Working Group.
- The deliverable D7.5 "Final Standardization Report" was submitted on schedule in September 2023. The document describes the standardization activities and results of the project partners within the organizations Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C), and also provides a description of how such organizations operate and of their process.
- Continued strong social media and project website presence, resulting in the following communication numbers for the whole project duration: more than 37k visitors and 85k visits to the website, more than 120 followers and 750 tweets in Twitter, more than 60 followers in LinkedIn and 16 videos and more than 360 views in YouTube.
- 19 industrial meetings participated with dissemination and exploitation focus (23 in total during the project), including key notes, panel discussions and seminar presentations in key international conferences related to the technology and solutions developed in the SIFIS-Home
- Participated in the key dissemination and exploitation event of the SIFIS-Home project, the IoT Solutions World Congress & Cybersecurity Congress in Barcelona 31.1.-2.2.2023, jointly with other projects funded under the same call to increase the reach and impact of the activity. 1 press release delivered and 1 interview given during the event.
- Delivering D7.6 “Final Business and Commercial Exploitation Plan” submitted on schedule September 2023. The final Business Plan included the analysis of Key Expoitable Results (KERs) of the project and their exploitation and impact potential, as well as a specific business and exploitation plan for the main result of the project, the SIFIS-Home Framework, including sustainability and monetizing plans. The analysis of market, competitors and market potential was revised. Furthermore, partners have updated and elaborated their individual exploitation plans to ensure effective exploitation of the solutions developed in the project.

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
MS4 - Testbed Deployment	This milestone will be considered reached after the successful deployment of the testbed to be used to implement and subsequently test the functionalities of the SIFIS Home architecture.	WP5, WP6	M20 (31/05/22)	M20 31/05/22	Deliverable D5.1 First version of SIFIS-Home testbed submitted.
MS5 – Final Component Design and First Implementation	This milestone will be considered reached after the final architecture has been defined, implementing the requirements collected in the second iteration (D1.2) and the deployment of the architecture on the testbed has been performed and these two activities have been reported in D1.4 and D5.2.	WP1, WP2, WP3, WP4, WP5, WP6	M24 (30/09/22)	M24 (30/09/22)	Deliverables D1.4 Final Component, Architecture, and Intercommunication Design and D5.2 First version of SIFIS-Home Security Architecture Implementation both submitted.
MS6 - Completed Initial Validation	This milestone will be considered reached once the first iteration of the validation has been performed, through the definition of the GQM and modes of verification for functional and non-functional requirements.	WP2, WP5, WP6	M30 (30/03/23)	M30 (30/03/23)	Deliverable D5.3 has been submitted.
MS7 - Final Implementation and Deployment of the Architecture	This milestone will be considered reached once the final SIFIS-Home framework and SIFIS-Home architecture are implemented and integrated in the testbed.	WP2, WP3, WP4, WP5, WP6	M33 (30/06/23)	M33 (30/06/23)	Deliverables D3.3, D4.3 and D5.4 have been submitted.
MS8 - Final Validation of the Pilot Use Case	This milestone will be considered reached once all the acceptance tests for use cases and the verification tests for functional and non-functional requirements have been completed, executed in the use case and the provided testbeds.	WP5, WP6	M36 (30/09/23)	M36 (30/09/23)	Deliverable D6.4 has been submitted.

Progress per Task

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

The activities of this task in Period 2 have concerned the management of the internal review, formatting and submission of deliverables D1.4, D2.1, D2.3, D2.4, D2.5, D2.7, D3.3, D4.3, D5.1, D5.2, D5.3, D5.4, D6.1, D6.2, D6.3, D6.4, D7.4, D7.5, D7.6, D8.3. All these deliverables have been submitted on time. Also, this task involved

the management of the updating and resubmission of deliverables which were reopened following the review meeting.

Task 8.2: Manage legal, contractual, financial, ethical and administrative matters (M1-M36/IC)
The Period 1 technical report was drafted and – following the midterm review – updated, submitted and successfully accepted by the EC together with the checked financial statements.

A grant amendment was prepared to replace MIND with DOMO and accepted by the EC on 09/08/2022. DOMO was allocated the remaining tasks, deliverables and budget originally given to MIND.

A grant amendment was prepared to split WITHSECURE OYJ into WITHSECURE OYJ and F-SECURE OYJ, which was admitted by the EC on 20/09/23. F-SECURE OYJ was assigned leadership of WP1 and WP7

Task 8.3: Ensure communication between partners (M1-M36/CNR)
The activities of this task have concerned maintaining the collaboration platforms - to work on the project and ensure regular meetings - 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 five plenary meetings, which have been held as primarily physical events in Helsinki, Munich, Rome (twice) and Stockholm.

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 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 plenary sessions. During the steering committee meetings, each WP leaders has provided a brief status report for their WP and highlighted any particular issues.

Contribution per partner to WP8

Partner	Contribution
CNR	Organization of steering committee meetings. Organization of physical, virtual and hybrid plenary meetings. Preparation of grant amendments and contribution to M27 technical report and D8.3.
ERI	Participated to the steering committee, review and plenary meetings.
FSEC	Participated to all plenary consortium meetings and steering committee meetings and WP leader meetings and organization of plenary meeting in Helsinki. Provided input to management and progress reports.
INT	Participated to the mid-term review and technical review meetings, all plenary consortium meetings and steering committee meetings and WP leader meetings and organization of plenary meeting in Munich.
IC	Participated in the mid-term review and technical review meetings, plenary consortium meetings, steering committee meetings, and WP leader meetings; led preparation of Period 1, M27 and Period 2 technical reports. Supported preparation of two grant amendments to replace MIND with DOMO, and to split WITHSECURE OYJ (FSEC) into WITHSECURE OYJ (FSEC) and F-SECURE OYJ (FSC).
LUM	Participated to the steering committee, review and plenary meetings.
DOMO	Participated to the Plenary meetings in Munich, Stockholm and Rome and to the steering committee meetings and WP leader meetings.
RIO	Participated to the steering committee, review and plenary meetings.
SEN	Sensative participated in all WP8 activities like monthly steering meetings and plenary meetings as well as doing all the expected reporting.

RISE	Participated to the mid-term review meeting, the additional technical review meeting, plenary consortium meetings, steering committee meetings, and WP leader meetings; provided input to management reports.
CEN	Participated to Project Steering Committee meetings and Plenary meetings.
POL	Participated to the Project Steering Committee meetings. Participation to the WP leader meeting and organization of the plenary meeting in Torino. Reviewed assigned deliverables. Participated to the Plenary meetings at Torino, Helsinki, and Munich.

Achievements

During the reporting period, the following have been achieved:

- Period 1 technical report was submitted and accepted by the EC together with the financial statements.
- M27 technical report was submitted and accepted by the EC.
- Period 2 technical report was submitted.
- Grant amendment successfully negotiated to replace MIND with DOMO.
- Grant amendment successfully negotiated to split WITHSECURE OYJ into WITHSECURE OYJ and F-SECURE OYJ.
- Project steering committee meetings have been held regularly on the second Thursday of each month.
- Five plenary sessions have been held.
- All project deliverables due by M36 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. Update of the plan for exploitation and dissemination of result (if applicable)

2.1 Exploitation

The situation with respect to the SIFIS-Home partners' exploitation plans in the DoA remain unchanged:

Consortium Partner	Exploitation Plan
CNR	CNR is the main public research organization in Italy. The results and the knowledge acquired in research projects have two major drivers for exploitation. CNR is in fact interested in increasing both research and innovation capabilities. Smart Home security is a relevant topic and the participation to the SIFIS-Home project will enable CNR to acquire new knowledge on this topic, together with giving the possibility to exploit and improve the current knowledge and expertise on intrusion detection, trust and policy management, which are core research topic of the Trustworthy and Secure Future Internet research group, involved in this project. Also, CNR will exploit the intermediate and final results of the SIFIS-Home project in parallel and future research and innovation projects, as well as exploiting technological results through possible spin-off activities.
ERI	Ericsson intends to exploit the project results mainly through the use of global standards, in particular IETF standards, and the open source code implementing the lightweight cybersecurity technologies developed in the project, applied to 5G and other 3GPP standardized connectivity solutions which are part of our product portfolio, and through collaborations and joint research and dissemination activities with industry partners and research institutes. In December 2022, Ericsson divested its IoT Accelerator platform which was previously part of the exploitation plan.
FSEC	FSEC exploits the project results to its connected home security offering, in particular, the F-Secure Sense router SDK. The offering is provided to router makers and service providers to embed the SENSE router SDK into their own routers. FSEC is currently protecting tens of millions of consumers through our 200+ service providers and telecom partners and the project results are exploited to the customer and partner bases. Therefore, integration of the project results to Sense router SDK improves IoT security and privacy of the large customer base globally.
INT	INT has strong focus at innovation capabilities related to ML and IoT topics. Beside support of Open source contributions INT plans to improve components used in the project in order to achieve best possible performance and richness of the feature set. Outcomes and feedback of the project will be taken to improve quality of each particular component, so such back-to-product contributions will have wider and longer by time impact through the industry, our partners and developers.
IC	IC are specialised in managing R&D and innovation projects. The company expects that successful support for the SIFIS-Home project will stimulate further project management assignments.
LUM	LUM is a small Italian SME. It focuses on system development and safer implementation opensource libraries ranging from multimedia to network protocols and offers consulting and training on those topics. Its current focus is on the Rust language as a mean to enforce best software engineering practices.
DOMO	DOMO is a new company which aims at making the new smart home technologies accessible to everyone, secure and trustworthy. The expected results of the SIFIS-Home project are a key exploitable result for DOMO. DOMO provides a distributed smart home solution that uses different devices. For these devices, reliability of the software framework and replication of functionalities is extremely relevant. Thus, DOMO aims at exploiting at the fullest the research results of the SIFIS-Home project, integrating them in its software framework, to include by design security, reliability and trustworthiness, which will become key value propositions of the DOMO product.
Riots	Riots wants to be actively involved in the development of security in IoT. As an innovative and agile SME IoT company, Riots is interested in finding out different larger scope possibilities in the field of IoT security and regards this project as a great opportunity to examine larger scale open source solutions. As Riots views IoT security as a rising central topic in smart homes and other similar infrastructures, the company firmly supports new and forthcoming established open source solutions in IoT security. It is in our interest to develop and offer functioning, secure, and reliable IoT solutions for wide commercial use. Riots is especially interested in the concept and implementation of privacy within a smart building

	– a large entity with a vast number of smaller components and several levels of users. The challenge of secure and correct distribution of rights to access different sets of the collected data and how to ensure the integrity of the network as a whole against malicious actions is one of our main focus points. In addition to strengthening our own product security, Riots wants to be involved in creating best practises and quality standards when it comes to IoT security.
SEN	SEN intends to incorporate the results from the project into Yggio, but also into own sensors, gateways and services when applicable. We will also actively promote the tools to our ecosystem of service providers. SEN has both municipalities, utility companies, real estate companies and home builders as customers and 15-20 service provider partners in domains as smart home, smart building, waste management, smart agriculture, sustainability reporting and smart shipping.
RISE	RISE is a research institute and will produce R&D know-how, specifications and software components as project results. Exploitable results include preventive/reactive cybersecurity lightweight solutions and their preliminary assessment through related proof-of-concept SW implementations; their transfer to project demonstrator/pilots; related standard proposals submitted and considered within the international open standardization body Internet Engineering Task Force (IETF). Also after the end of the SIFIS-Home project, RISE will exploit the project results according to a research exploitation model, which includes: dissemination of research and development results through academic publications; contribution to open standardization activities, with particular reference to the international body IETF, as in turn expected to indirectly contribute towards other international standardization bodies that rely on IETF standards as building blocks to develop their specifications (e.g., Open Mobile Alliance and 3GPP); integrating software components into related R&D activities as well as official open-source software libraries, with particular reference to the open-source library Californium from the Eclipse Foundation; establishing and reinforcing collaborations for joint research and dissemination activities; enhancing competence and expertise in cyber security, with particular reference to the IoT and smart environment application/network domains; and participating in future research and innovation projects within IT-security areas. In addition to RISE itself, the results from the exploitation actions mentioned above are intended to benefit and target especially the "IoT industry" and the "Research community" as relevant customer segments.
CEN	CEN will use its Cyber Security lab facilities for developing and piloting the developed solution. The aim of CEN's research is to develop expertise for companies and organizations, in order to enhance their activities and competitiveness. The goal is to both provide and create new knowledge, skills and technologies for the local businesses and industries. In this project the Cyber Secure team working with A.I. development, wireless communication and sensor-related technologies are heavily involved. CEN will use these project outcomes to improve its knowledge for future applications.
POL	With over 26,000 students, POL is the second largest technical university in Italy. The workforce dedicated to research and teaching includes around 900 Professors, 700 PhD Students and 300 Research Assistants, covering all major areas of the engineering and architecture disciplines. Participation in the SIFIS-Home project will enable POL to acquire new knowledge on this topic, and to promote technology transfer to SMEs in the region with its dedicated office in charge of technology transfer activities. Also, POL's participation will help improve the quality of teaching: advanced courses on software engineering, ambient intelligence, data management, taught by the faculty involved in SIFIS-Home will use these concepts and software services for lab exercises as well as for projects and theses.

2.2 Standardisation

Building on a long-term experience and successful track record, RISE and Ericsson have been extensively engaged in standardization activities under the international body Internet Engineering Task Force (IETF), especially in the Working Groups "CoRE" [STD-CORE], "ACE" [STD-ACE], "LAKE" [STD-LAKE] and "SCHC" [STD-SCHC].

This mostly consists in writing, progressing and presenting technical specification documents as standard proposals in the form of Internet Drafts, where RISE and Ericsson are main contributors and co-authors, often jointly. The full list of relevant IETF Internet Drafts is available in the project website at [7.2-LIST]. These standard proposals are often supported by proof-of-concept implementations that undergo interoperability tests.

RISE and Ericsson regularly and actively participate in IETF meetings, virtual IETF Working Group interim meetings and other related events, such as IETF Hackathons and interoperability tests. Marco Tiloca (RISE) is Chair of the Working Group "CoRE", as well as reviewer in the IoT Directorate and the ART Area Review Team. Francesca Palombini (Ericsson) is Area Director for the "Application and Real Time" (ART) Area, which includes also the "CoRE" Working Group among others.

Besides continuing its effort and engagement in standardization activities within the IETF body, the consortium has also been involved in standardization activities within the World Wide Web Consortium (W3C) [7.2-W3C].

Specifically, Luminem has been involved in the W3C Web of Things (WoT) Community [7.2-WOT], where it is now a full-fledged member and has been active within the WoT Interest Group, Community Group and Working Group [7.2-WOT-WG]. The contribution in W3C WoT is related to the activities carried out in WP2, and concerns the overhaul of the Thing Description 2.0 information model, in particular regarding the WoT-Profile and the Protocol Bindings Templates to address the concerns on describability, ultimately to ensure semantics interoperability of the used information models. Furthermore, Luminem contributed with a from-scratch Rust implementation of WoT standards, also integrating the SIFIS-Home Risk/Hazard labels in simulated things.

Further details especially pertaining to the period covered in this technical report are provided in Section 1.2.7 as a summary about Task T7.2 "Standardization".

[STD-CORE] https://datatracker.ietf.org/wg/core/about/
[STD-ACE] https://datatracker.ietf.org/wg/ace/about/
[STD-LAKE] https://datatracker.ietf.org/wg/lake/about/
[STD-SCHC] https://datatracker.ietf.org/wg/schc/about/
[7.2-LIST] https://www.sifis-home.eu/index.php/standardization/
[7.2-W3C] https://www.w3.org/
[7.2-WOT] https://www.w3.org/WoT/
[7.2-WOT-WG] https://www.w3.org/WoT/wg/

2.3 Dissemination

The current status with respect to implementing the SIFIS-Home dissemination plan in the DoA is as follows:

Dissemination Channel	Dissemination Activity	Target Audience	Target Indicator	Achieved by the end of the reporting period
Project Website	Publish project summary, regular news and event updates on website.	Industry, Academia, Policy-makers, Standardisation bodies, Commercial users, General public.	10k individual users contacts on the web site	By month 36, there more than 37,000 visitors and 85,000 page views. Statistics are not available from the first 5 months of the website, because of the late installation time of the statistics plugin.
Project news	Publish project news releases and distribute through broader scientific news channels.	Industry, Academia, Policy-makers, Standardisation bodies, Commercial users, General public.	6 interviews, 8 press releases	5 interviews given to different magazines, incl. Wired Italy (www.wired.it), 1 joint press release together with other projects funded under the same call, 16 news articles

				published on the project website
Social media	Publish regular news and event updates.	Industry, Academia, Policy-makers, Standardisation bodies, Commercial users, General public.	More than 100 followers for LinkedIn, More than 100 followers for Twitter, More than 1000 tweets from account, 10 Videos on YouTube, More than 500 viewers.	64 followers on LinkedIn, 129 followers on Twitter, 750 tweets from account, 16 videos on YouTube, 384 viewers in total.
Technical and Academic publications	Publish results in international peer reviewed journals (e.g. ACM Transactions on Information and System Security).	Industry, Academia, Standardisation bodies, Commercial users	More than 20 conference/workshop Publications, More than 2 journal publications, More than 3 white papers	10 conference publications, 10 journal publications, 1 white paper
Conference participation (events)	Present results at international scientific conferences (e.g. ESORICS).	Industry, Academia, Standardisation bodies, Commercial users	12 or more academic conferences/workshop, 9 or more industrial meetings, 10 seminars given	7 workshops participated, 23 industrial events/meetings participated, 5 seminars given
Organisation of events	Present results during partners' workshops.	Industry, Academia, Standardisation bodies, Commercial users	At least 2 workshops organised/supported, More than 30 participants per event, At least 10 seminars organised	4 workshops organised with more than 30 participants per event, seminars organized

The partners have achieved the following scientific and outreach dissemination activities during the reporting period:

Type of publication	**Title**	**Authors**	**Venue**	**Year**
Article in Journal	Evaluating the Performance of the OSCORE Security Protocol in Constrained IoT Environments	Martin Gunnarsson, Joakim Brorsson, Francesca Palombini (ERI) , Ludwig Seitz (RISE) and Marco Tiloca (RISE)	Internet of Things; Engineering Cyber Physical Human Systems	2021
Article in Journal	Exploiting IFTTT and Usage Control Obligations for Smart Home Security and Management	Giacomo Giorgi, Antonio La Marra, Fabio Martinelli, Paolo Mori, Athanasios Rizos, Andrea Saracino (CNR)	Concurrency and Computation Practice and Experience	2021
Conference proceedings	On-demand Key Distribution for Cloud Networks	Nicolae Paladi, Marco Tiloca (RISE), Pegah Nikbakht Bideh and Martin Hell	24th Conference on Innovation in Clouds, Internet and Networks (ICIN 2021), Demonstration track	2021

Article in Journal	Privacy preserving data sharing and analysis for edge-based architectures	Mina Sheikhalishahi, Andrea Saracino, Fabio Martinelli, Antonio La Marra (CNR)	International Journal of Information Security	2021
Article in Journal	Using recurrent neural networks for continuous authentication through gait analysis	Giacomo Giorgi, Andrea Saracino, Fabio Martinelli (CNR)	Elsevier PR Letters	2021
Conference proceedings	Flowrider - Fast On-Demand Key Provisioning for Cloud Networks	Nicolae Paladi, Marco Tiloca (RISE), Pegah Nikbakht Bideh and Martin Hell	17th EAI International Conference on Security and Privacy in Communication Networks (EAI SecureComm 2021)	2021
Article in Journal	Preserving Privacy in the Globalized Smart Home:The SIFIS-Home Project	Luca Ardito (POL), Luca Barbato (LUM), Paolo Mori (CNR), Andrea Saracino (CNR)	IEEE Security And Privacy	2021
Article in Journal	Quality Assessment Methods for Textual Conversational Interfaces: A Multivocal Literature Review	Riccardo Coppola, Luca Ardito (POL)	MDPI Information	2021
Conference Proceedings	A Real-Time Deep Learning Approach for Real-World Video Anomaly Detection	Stefano Petrocchi, Giacomo Giorgi (CNR), Mario G. C. A. Cimino:	ARES 2021: The 16th International Conference on Availability, Reliability and Security	2021
Article in Journal	Performance Evaluation of Group OSCORE for Secure Group Communication in the Internet of Things	M. Gunnarsson, K. M. Malarski, R. Höglund and M. Tiloca (RISE)	ACM Transactions on Internet of Things	2022
Conference proceedings	An application of Netspot to Detect Anomalies in IoT	Tom Tuunainen, Olli Isohanni, Mitha Jose (CEN)	2022 IEEE 8th International Conference on Network Softwarization (NetSoft)	2022

Conference proceedings	Privacy vs Accuracy Trade-Off in Privacy Aware Face Recognition in Smart Systems	Wisam Abbasi, Paolo Mori, Andrea Saracino (CNR), Valerio Frascolla (INT)	12th Workshop on Management of Cloud and Smart City Systems (MoCS 2022)	2022
Article in Journal	Vulnerabilities of the 6P Protocol for the Industrial Internet of Things: Impact Analysis and Mitigation	F. Righetti, C. Vallati, M. Tiloca and G. Anastasi (RISE)	Computer Communications	2022
Conference proceedings	Privacy-Preserving Speaker Verification and Speech Recognition	Wisam Abbasi (CNR)	ETAA2022	2022
Conference proceedings	Demo: Usage Control using Controlled Privacy Aware Face Recognition	Arpad Müller, Wisam Abbasi (CNR)	12th Workshop on Management of Cloud and Smart City Systems (MoCS 2022)	2022
Article in Journal	Lightweight Authenticated Key Exchange With EDHOC	Mališa Vučinić; Göran Selander; John Preuss Mattsson; Thomas Watteyne (ERI)	Computer	2022
Conference proceedings	Secure Software Updates for IoT based on Industry Requirements	Ludwig Seitz, Marco Tiloca, Martin Gunnarsson and Rikard Höglund (RISE)	9th International Conference on Information Systems Security and Privacy (ICISSP 2023)	2022
ePrint Archive	On using the same key pair for Ed25519 and an X25519 based KEM	Erik Thormarker	Cryptology ePrint Archive, Paper 2021/509	2022

Conference proceedings	Key Update for the IoT Security Standard OSCORE	Rikard Höglund, Marco Tiloca, Simon Bouget and Shahid Raza (RISE)	2023 IEEE International Conference on Cyber Security and Resilience (CSR 2023)	2022
Conference proceedings	Research, Implementation and Analysis of Source Code Metrics In Rust-Code-Analysis	Luca Ardito, Marco Ballario, Michele Valsesia (POL)	The 23rd IEEE International Conference on Software Quality, Reliability, and Security (QRS 2023)	2023
Conference proceedings	The Explainability-Privacy-Utility Trade-Off for Machine Learning-Based Tabular Data Analysis	Wisam Abbasi; Paolo Mori and Andrea Saracino (CNR)	The 20th International Conference on Security and Cryptography - SECRYPT 2023	2023
Conference proceedings	Privacy-Preserving Object Recognition with Explainability in Smart Systems	Wisam Abbasi ; Paolo Mori and Andrea Saracino (CNR)	PriST-AI 2023	2023
Conference proceedings	Graph-Based Android Malware Detection and Categorization through BERT Transformer.	Marco Simoni; Andrea Saracino (CNR)	ARES 2023	2023
Article in Journal	An Artificial Intelligence-Based Approach to Detect the Quality of Wooden Panels using Convolutional Neural Networks	T. Tuunainen, O. Isohanni, M. Jose (CEN)	International Journal of Engineering Research in Computer Science and Engineering	2023

ePrint archive

Consortium Partner(s)	Title	Journal	Date
ERI	On using the same key pair for Ed25519 and an X25519 based KEM	Cryptology ePrint Archive, Paper 2021/509	2021

Industrial events

Consortium Partner(s)	Activity	Conference or Workshop	Date
INT	Industry Presentation	ICC 2022 / Industry Workshop #6: "Toward AI-native 6G Networks"	17.05.2022
INT	Invited Talk	6G Symposium Spring 2022	23.05.2022
FSEC	Exhibition booth	International Cybersecurity Forum	7.-9.6.2022
FSEC	Presentation	Broadband Forum's BASe at BREKO Fiberdays	13.6.2022
INT	Invited Talk	IoT Week 2022 / Session "IoT Intelligent Connectivity and Edge Computing Research Priorities"	20.06.2022
FSEC	Presentation & expo	SPECIES Conference	20.-21.9.2022
LUM	Presentation	Web of Things Online Meeting	22.9.2022
FSEC	Presentation	FISC & Kyberturvallisuuden EU-rahoitus	12.10.2022
CEN	Booth & expo	Centria DropIn	5.-6.10.2022
FSEC	Participant	Purple Foundation Summit 2022	20.10.2022
CEN	Seminar	SecTalk	13.12.2022
CNR	Presentation	SecTalk	13.12.2022
CEN	Seminar	FUI+Näringsliv - Valentine´s day business matchmaking event	14.2.2023
CEN	Expo	Vaasa EnergyWeek 2023 industry expo	24.3.2023
CEN	Expo	Wasa Future Festival	8.8.2023
CNR/CEN	Webinar	Increasing Cybersecurity and Empowerment in the Digital Environment in Europe	13.9.2023

Outreach

Partner(s) Concerned	Event	Audience	Date
RISE	RISE Computer Science Department Partner Event (former Open House)	Industry and academia	10.5.2022
SEN	Sensative Sense 2	IoT industry / Public invitation	18.5.2022
FSC	International Cybersecurity Forum	Cybersecurity industry	7.-9.6.2022
FSC	Broadband Forum's BASe at BREKO Fiberdays	Broadband industry and customers	13.6.2022
FSC	F-Secure SPECIES Conference	Consumer cybersecurity industry	20-21.9.2022
FSC	Prpl Foundation Summit 2022	Industry	20.10.2022
FSC	FISC & Kyberturvallisuuden EU-rahoitus	Cybersecurity industry	12.10.2022
RISE, ERI	Given the tutorial "Lightweight End-to-End Security using OSCORE and EDHOC" at the "IEEE 8th World Forum on Internet of Things"	Industry and Academia	26.10.2022

SEN	Sensative Yggio Days 2022	IoT industry / Customers and Partners	22-23.11.2022
CEN	SECTalk	Academia and industry	31.12.2022
RISE, ERI	Given the lecture "Application Layer Security for Constrained Devices with OSCORE and EDHOC" at the cycle of guest lectures for the University Course "Cyber Security II: Specialisation" of Tampere University	Academia and Research Community	23.2.2023
RISE	Given the seminar "Secure End-to-End (Group) Communication for the IoT" at the series of internal seminars of IMT Atlantique	Academia and Research Community	1.6.2023
RISE	Given the invited talk "IETF Standardization of Lightweight Security Protocols for the IoT" at the Standardization Workshop of the European Commission H2020 project CYRENE	Industry and Academia	16.6.2023
RISE	RISE Computer Science and AI Open House	Industry and Academia	14.9.2023

3. Update of the data management plan (if applicable)

Data management has been covered as part of the submitted deliverable D2.6. In particular, the deliverable has covered all the aspects related to GDPR and provided guidelines which are valid both for third-party developers and for the project activities itself. Up to now we have not covered yet the data management plan related to data acquired during showcase activities. The ethical board has been set-up following the review meeting and is composed by two legal experts: Mr. Marco Ciurcina and Mr. Giacomo Conti affiliated with POL. The ethical board has conducted in the last months dedicated meetings with the WP leaders to inquire on the data types managed or produced by the WP activities, to identify potential ethical issue. An addendum to D2.6 has been prepared to report this analysis and suggested or enforced measures

4. Follow-up of recommendations and comments from previous review(s) (if applicable)

4.1 Recommendations concerning Period 1

In the review report for Period 1, the project reviews indicated the results provided by the SIFIS-Home consortium were mainly accepted, however there were some aspects of the delivered work that need to be corrected. They then provided the following thirteen (13) recommendations to the SIFIS-Home consortium:

R1. Progress of the objectives is presented in a WP basis. The project objectives are not measured and there is no link provided between WP objectives and project objectives. To understand the progress of the project an adequate matching has to be provided following a SMART approach.

SIFIS-Home consortium's response
At the end of each objective in the management report (D8.2), a summary was added indicating the progress towards achieving the objective.

R2. There is not a clear matching between the requirements and the architecture components, it has to be clearly linked as it will help prioritization in the developments. The Project is recommended to clarify in a revision to the relevant deliverable the mapping between the requirements elicited and the architectural design.

SIFIS-Home consortium's response
We thank the reviewer for raising this point, which has been one of our main concerns immediately following the mid-term review meeting. The comment has been addressed as requested, by mapping all the components with the requirements in deliverables D1.3 and D1.4.

R3. When a WP does not have an associated deliverable during the period it would be advisable to provide detailed information about the developed work. The periodic management report can serve as a collector of information not suited to be included in deliverables planned for the review period.

SIFIS-Home consortium's response
This was done for the management report (D8.2).

R4. The market assessment needs more affinity with the real market.

SIFIS-Home consortium's response
Further assessment provided in the resubmitted report D7.3.

R5. Plans in WP7 do not providing paths for creating impact in any of the axes proposed in the WP.

SIFIS-Home consortium's response
Further details and clarification added in the resubmitted report D7.3.

R6. Risk management needs to be reported adequately. There is only a risk list and no described procedure. PPR may need to have this information provided.

SIFIS-Home consortium's response

During Period 2 greater attention will be paid on whether risks have occurred and mitigation measures applied as well as providing a commentary on the state of play.

R7. Impacts are not analysed in the PPR, this is part of the PPR template.

SIFIS-Home consortium's response
It was too early at the end of Period 1 to comment on progress towards achieving the Expected Impacts indicated in Section 2.1 of the Description of Action. However, an analysis is foreseen to be made at the end of Period 2 in the periodic technical report.

R8. In the event the Project intends to demonstrate the said Parental Control technologies in a pilot, the Project may want to consider requesting a project amendment so as to give SIFIS-HOME the required ethics management and reporting to the EC.

SIFIS-Home consortium's response
The parental control will not be used in the pilot, though a specific analytic able to perform this analysis has been provided. However, we have extended the dedicated WP2 deliverables with ethical considerations and privacy issues to face when using images and other multimedia involving people and children. Furthermore, we have prepared and included consent modules to be signed by any person, inside or outside the consortium, whose image could be used in the SIFIS-Home project.

R.9. The project is recommended to clarify what provisions exist in the SIFIS-HOME APIs and architecture to manage the cryptographic key material, so as to mitigate the risk that the said key material may suffer from key recovery attacks. This clarification shall consider the relevant key materials (e.g., Master Secret and Master Salt in the OSCORE Security Context) both before and after the rekey operations.

SIFIS-Home consortium's response
Following the review meeting, this point has been clarified by inserting the requested information in deliverables D1.3 and D1.4.

R10. It should be clearly explained what tools and metrics SIFIS-HOME will use/incorporate. And emphasize which tools will help security-wise.

SIFIS-Home consortium's response
We thank the reviewer for this comment. Tools exploited by the SIFIS-Home components have been referenced in the relevant deliverables.

R11. The workflows do not include dependency analysis tools.

SIFIS-Home consortium's response
The SIFIS-Home defined workflows are not dependent one from the other. In fact, all workflows describe atomic operations

R12. The management report (D8.2), in section 1.1, needs to include a summary of the activities carried out towards the achievement of each objective. Right now, it includes the objective and the success criteria. It has to include, in addition to the objective and success criteria, the progress of the work performed affecting that objective. D8.2 needs to address the status of the self-healing feature mentioned in the DoA.

SIFIS-Home consortium's response
At the end of each objective in the management report (D8.2), a summary was added indicating the progress towards achieving the objective.

R13. Resubmission of D1.3, D7.3 and D8.2 addressing the requested modifications, has to be done 2 months after the reception of the consolidated evaluation report.

SIFIS-Home consortium's response
The updated three deliverables were resubmitted within two months of receiving the consolidated evaluation report.

4.2 Recommendations concerning Period 2

In the review report for Period 1, the project reviews indicated the Period 2 activities should focus on the completion of the developments in the different WPs and the integration in the SIFIS-HOME final solution. They then provided the following fifteen (15) recommendations to the SIFIS-Home consortium:

R1. US and UC are clearly presented however the consortium needs to link them with the real market and current application domains, e.g. Active and Healthy aging, please check ACTIVAGE project.

SIFIS-Home consortium's response
We thank the reviewer for this comment. We are inserting a novel section exploring potential markets for SIFIS-Home related products with a potential link to the proposed use cases. The paradigm explored and developed in SIFIS-Home can, in fact, easily apply to smart living environments, aiding aging people. The resilience and privacy management aspects of the SIFIS-Home project should imply an increased reliability and availability of the system to make it able to handle potential emergencies or assistance request, without the risk of the single point of failure. Through this action, we are also addressing the request for a deeper market analysis.

R2. Standardization needs a broader focus, and the consortium needs to address other SDOs out of IETF. For example, interoperability, security, data modelling, and specifically application domains.

SIFIS-Home consortium's response
Besides continuing its effort and engagement in standardization activities within the IETF body, the consortium has also been involved in standardization activities within the World Wide Web Consortium (W3C).

Specifically, LUM has been involved in the W3C Web of Things (WoT) Community, where it is now a full-fledged member and has been active within the WoT Interest Group, Community Group and Working Group.

The contribution in W3C WoT is related to the activities carried out in WP2, and concerns the overhaul of the Thing Description 2.0 information model, in particular regarding the WoT-Profile and the Protocol Bindings Templates to address the concerns on describability, ultimately to ensure semantics interoperability of the used information models. Furthermore, LUM contributed with a from-scratch Rust implementation of WoT standards, also integrating the SIFIS-Home Risk/Hazard labels in simulated things.

R3. Improve industrial dissemination. Scientific academic dissemination is on the good path, however more participation in trade fairs, industrial events and demo fora will be required during next period (e.g. IoT Week)

SIFIS-Home consortium's response
In total 23 industrial events have been participated and the list of events is reported in D7.6. SIFIS-HOME project joined the joint dissemination and exploitation event IoT Solutions World Congress & Cybersecurity Congress in Barcelona 31.1.-2.2.2023 together with the other 4 projects funded under the same call with a shared booth and project specific stands at the exhibition area. Demonstrations developed within the project were showcased during the exhibition. A joint press release was also delivered during the event together with projects under the same call.

R4. WP7 may require to stress community building, success of the project results exploitation will depend on the interest of third parties in SIFIS-HOME utilization. Links with DIH, developers, project clusters and open source communities (e.g. ECLIPSE KURA) need to be planned.

SIFIS-Home consortium's response
The project has emphasized the existing community building activities, especially in the following communities:

- Rust: Members of both LUM and CNR are contributors to the core Rust compiler and standard library and authors of widely used tools. Part of the work in SIFIS-Home had been shared back, in particular bugfixes for issues found during the SIFIS-Home development.
- WoT: LUM is actively taking part in the Community Meetup and is helping with their organization, the wot-rust implementation has been presented to both the Web of Things at its first Community Meetup and the Rust community at Rustlab 2022.
- Eclipse Californium: RISE is an official contributor to the open-source framework Eclipse Californium from the Eclipse Foundation, which already includes the RISE implementation of the OSCORE security protocol.IETF (Internet Engineering Task Force): RISE is a key contributor in the international and open standardization body IETF.FIWARE Community: Sensative has during the project execution set up the FIWARE OiL - Open IoT labs Hub in its office in Lund to facilitate the cooperation and community building between industry partners working with FIWARE.AIxIA (Italian Association for Artificial Intelligence): Created a working group on cybersecurity and AI working on WP4 topics. CNR leads the working group.

R5. Exploitation needs improvement, there is no identification of KERs and joint exploitation has not been presented. There is no business plan included. E.g. analyze the possibility of exploiting the whole SIFIS-HOME solution. This aspect of the project presents some weaknesses.

SIFIS-Home consortium's response
The identification of KERs, description of the joint exploitation and business models related to the exploitation of the SIFIS-Home solution have been presented in the resubmitted D7.3 and further developed in D7.6, including the analysis of the exploitation and impact potential of KERs. D7.6 includes of business plan and the exploitation of the whole SIFIS-Home solution has been analysed and planned in further detail.

R6. Architecture is not linked with the requirements. The different components of the architecture should emanate from the requirements elicitation

SIFIS-Home consortium's response
We thank the reviewer for this comment. We have addressed it as suggested by adding a section and a table reporting the link between requirement and SIFIS-Home Framework components in the resubmitted D1.3, and updated it in D1.4 for the newly defined/refined components.

R7. APIs are very preliminary and more attention has to be devoted to the data models and semantic interoperability, e.g. ONTOCOMONS or ETSI SAREF.

SIFIS-Home consortium's response
We thank the reviewer for this comment. We have fully re-defined the APIs by following a specific custom ontology. The new set of APIs, with the ontology definition, is available in D1.4.

R8. The project is recommended to clarify what measures exists in the SIFIS-HOME APIs and architecture to securely operate SIFIS-HOME devices which are not received any longer security updates from their manufacturers (i.e., their shelf-life is shorter than their lifetime, due to various forms of obsolescence).

SIFIS-Home consortium's response
This aspect is not in the scope of the SIFIS-Home project as the SIFIS-Home framework is planned to be device independent. More in detail, the SIFIS-Home framework, comes as an application which can be installed on any capable device. The SIFIS-Home framework is thus not dependent upon the device firmware and though - to increase security - a module could be added to verify if the installing device matches specific security standards (including the updated version of a firmware), this is not an aspect on which the project is focused.

R8. In M18 of the project there is a lack of description of testing activities, clarification on the three defined testbeds is needed.

SIFIS-Home consortium's response

We thank the reviewer for this comment. Clarification on this point will be provided via WP5 and WP6 upcoming deliverables. More in details, we have deployed an emulated testbed implemented through a set of Virtual Machines which emulate the smart devices connected in a SIFIS smart home environment. The Virtual Machines install a deployment of the various SIFIS-Home framework components. A second testbed is the simulated testbed. This testbed uses general purpose devices, in particular Raspberry-PIs, to simulate smart devices and their integration with NSSD actuators. These two testbeds are a result of the WP5 activities. Finally, the real testbed is provided by the pilots, where SIFIS-Home is integrated in real ready-to-market devices provided by DOMO, RIOTS and CENTRIA. This is a result of WP6 activities.

R9. Appoint an innovation manager to handle the issues related with innovation management within the project. Although there are innovation management procedures in place, the success of these measures in M18 are not sufficiently demonstrated.

SIFIS-Home consortium's response

We thank the reviewer for this comment. The innovation manager for SIFIS-Home is represented by the WP7 and exploitation leader, in the persons of Tuuli Lindroos and Sini Olkanen from FSEC, who has coordinated, with the cooperation of ERI, DOMO and CNR, in the past months the activities of business modelling and preparation of a business plan for a potential SIFIS-Home product.

R10. PPR should follow the template and In future Period Reports and Management Reports the Project is recommended to discuss in detail the use of resources, highlighting and explaining deviations, if any, between the actual and planned resources per work-package and for each Beneficiary in the Grant Agreement. The discussion shall contrast the efforts invested to the efforts committed per project partner and for work-package, and the budget spent to the budget allocated.

SIFIS-Home consortium's response

The Period 1 technical report discussed in detail the use of resources, highlighting and explaining deviations between the actual and planned resources per work-package and for each beneficiary. However, the original version of deliverable D8.2 "Period 1 Management Reports" did not contain this information, because it had a due date immediately at the end of Period 1 (31/03/22) which did not allow partners sufficient time to provide their costs and person-months. In the updated version of D8.2 resubmitted on 12/08/22, a description of the use of resources was added.

R11. Deliverables should not repeat prose from previous deliverables. For example, D1.2 repeats a lot of prose from D1.1. Only the changes with respect to D1.1 should have been included. Section 3.3. of D7.3 does not contribute to the core topic of the deliverable. WP3 provided feedback to WP1, but that feedback should not be included in D3.1 (unnecessary). Only the result of that contribution should have been documented in the deliverables for WP1. For future deliverables, if some content from a previous deliverable is included, it should be shown using a different color, or font.

SIFIS-Home consortium's response

A: We thank the reviewer for this comment. We wanted to keep deliverables as a self-contained document. The re-use of material from one deliverable to the other, normally happens when there are preliminary and final deliverables. We will provide, for review purposes, separated deliverables with differently colored text as suggested.

R12. Quality control has to be improved and proof reading put in place, some deliverables are written in a sloppy way, and lacked a final review. For example, the sections on Ratatosk in D1.3 are difficult to read because of how they are written.

SIFIS-Home consortium's response

A: We apologize for this and we will put more attention to the upcoming deliverables. Ratatosk section has been rewritten in D1.3 and D1.4.

R13. As for dissemination/communication activities, include quantitative information of the use/effectiveness of Twitter, LinkedIn, and YouTube. Include statistics of the number of web page visits.

SIFIS-Home consortium's response
The quantitative information has been added to the technical reporting and will be more clearly presented in the D7.4 report.

R14. To submit a preliminary version of D7.6 regarding business models and exploitation.

SIFIS-Home consortium's response
The business models and elaborated version of the exploitation activities have been included in the resubmitted D7.3 report, and business planning and exploitation of the project's key results has further developed for D7.6.

R15. Regarding WP4, the research-related contributions beyond the state of the art and existing technologies should be explained in detail in the future D4.3. Also, for those contributions, a complete analysis and design of the new algorithms/ tools/solutions should be documented and demonstrated.

SIFIS-Home consortium's response
We thank the reviewer for this comment. Deliverable D4.3 will include technical descriptions and research results with a deeper technical level, extracting material directly from the published or ongoing research papers. Furthermore, we are providing as appendix to this document a summary document of the research activities performed for WP2, WP3 and WP4, with a focus on the activities for intrusion detection, and with a description of the research relevance or application for SIFIS-Home.

4.3 Recommendation following second review meeting

R1. A mapping between the MIND solutions and the DOMO solutions is needed. That should be included in D6.2.

SIFIS-Home consortium's response
The mapping has been performed in the resubmitted version of D6.2, where we have also included an appendix for easy-to-read mapping of how the MIND architecture has been translated in the DOMO architecture.

R2: Many of the results of WP3 will not be included in the final pilots. So those are not part of the SIFIS-Home solution/ product. The deliverables should include *only* the contributions that will be part of the global SIFIS-Home solution/ product. The results that will be included in that final SIFIS-HOME product should be shown.

SIFIS-Home consortium's response
A larger integration effort has been performed with the goal of providing a fully integrated solution with more elements from WP3 which were not previously integrated. Deliverable 3.3 has been modified as requested.

R3. Explain how the SIFIS-HOME solution will be dealing with non-IP devices, as currently this seems to be a vulnerability.

SIFIS-Home consortium's response
Following the reviewer's request, an analysis of the possible non-IP devices has been conducted in order to understand if they can affect the system security. Out of this analysis, we have assessed that the non-IP devices are not in the scope of the SIFIS-Home project as their communication mechanisms does not follow the description of neither Smart Devices or Not So Smart Devices. We are still aware that such devices, as external elements outside of the SIFIS-Home architecture, can potentially performs attacks over the wireless channel. All attacks against cryptography would be not effective, as all communication are TLS protected. On the other hand, it is still possible that such devices attempt to jam the channel, breaking up wireless communications. Resilience to such attacks would completely depend from design choice at channel level. Such dimension has not been considered in the SIFIS-Home project as they fall mainly in the telecommunication engineering scope, which is not part of the skills of the SIFIS-Home consortium.

R4. In the final review the reviewers would like to see a real live demonstration. That demostration/demontrations should include all the results of the project.

SIFIS-Home consortium's response

This comment has been addressed as requested. After integrating the SIFIS-Home framework in the DOMO use case, for validation we run a set of live tests to validate the functionalities of the SIFIS-Home framework in a fully integrated manner. The integration effort done in WP5 and WP6 has been valued through the performed validation experiments. In particular, for each use case defined in D1.2, we have demonstrated the full execution of the workflows, involving all of the SIFIS-Home framework components and SIFIS-Home architecture device. The majority of the use cases involve at least 3 smart devices, interacting with 3 NSSDs , one laptop and one mobile phone installing the SIFIS-Home Mobile Application. We made the demonstrations available to the reviewers in a dedicated folder. All videos have been recorded live, with no interruptions or "director's cut", to demonstrate the complete integration. Together with use case videos, spanning already the majority of the SIFIS-Home framework components, more videos have been recorded to demonstrate integrated interactions of the components whose functionalities have been previously demonstrated as standalone. A specific attention has been given to components derived from WP2 and WP4 activities. All demos have been performed directly in the DOMO use case.

R5. The exploitation plans need to include plans to exploit the *global* SIFIS-Home solution/product.

SIFIS-Home consortium's response

We thank the reviewer for this comment. As part of the activities of the WP7, following the former review meeting, we have analyzed all the Key Exploitable Results of the SIFIS-Home project, to assess their level of innovation and potential impact. Furthermore, in the resubmitted version of D7.3 we have proposed three business models for potential SIFIS-Home derived products. The SIFIS-Home framework and architecture is pretty complex and it is difficult to derive a single specific product, unless discussing a commercial model which must be handled by a foundation, similar to the AOSP (Android Open Source Project), who handles the set of sub-products, proposing different, still interlaced business models, targeting respectively device producers, application developers, smart home tenant and smart home system installers. We did our best to convey this view in a high level business plan for a SIFIS-Home prospective product in D7.6.

R6: Self-healing needs to be addressed (and demonstrated) in the final review

SIFIS-Home consortium's response

We thank the reviewer for this comment. The self-healing has been addressed by means of the implementation of the Node Manager functionalities. The Node Manager exploits a voting procedure based on a mechanism for distributed trust, which enables the SIFIS-Home framework to identify misbehaving nodes and removing them from the system. Once a node is removed, the DHT is reconfigured to be able to work with a lower number of smart devices, reassigning the control of the NSSDs previously communicating with the removed nodes, to the remaining ones. These aspects of the self-healing feature have been demonstrated in the demo of Use Case 18 and Use Case 19.

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

5.1 Tasks

There were no significant deviations in tasks during Period 2. All deliverables were submitted on schedule and accepted by the EC project officer and external reviewers.

5.2 Use of resources

It was not feasible to have the consortium partners' Period 2 costs and efforts (person-months) on the last day of the Period 2 reporting period when deliverable D8.3 was due i.e. 30th September 2023.

Instead, the consortium partners' Period 2 costs and efforts will be reported in their financial statements in the EC's portal (SyGMa) within 60 days of the end of the reporting period for Period 2 (i.e. by 30th November 2023) in accordance with Article 20.3 of SIFIS-Home grant agreement.