
D7.6

# Final Business and Exploitation Plan

## WP7 – Dissemination, Standardization and Exploitation

**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

***30/09/2023***
***Version 1.0***

*Responsible partner: FSC*
*Editor: Sini Olkanen*
*E-mail address: sini.olkanen@f-secure.com*

| **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-2-2020#952652*

**Authors:** Sini Olkanen (FSC), Tuuli Lindroos (FSC), Marko Komssi (FSC), Andrea Saracino (CNR), Göran Selander (ERI), Valerio Frascolla (Intel), Giles Brandon (IC), Luca Barbato (LUM), Domenico De Guglielmo (DOMO), Samuli Stenudd (RIO), Håkan Lundstöm (SEN), Marco Tiloca (RISE), Laura Palovuori (CEN), Luca Ardito (POL)

**Reviewers:** Marco Tiloca (RISE), Valerio Frascolla (INT)

**Revision History**

| Version | Date | Name | Partner | Section Affected Comments |
|---|---|---|---|---|
| 0.1 | 19/10/2022 | Initial ToC | FSC | All |
| 0.2 | 16/8/2023 | Updated TOC | FSC | All |
| 0.7 | 11/09/2023 | Updated text | All | All |
| 0.8 | 18/09/2023 | Ready for review | FSC | All |
| 0.9 | 22/09/2023 | Internal review | RISE & INT | All |
| 1.0 | 27/09/2023 | Ready for submission | FSC | All |

## Executive Summary

The SIFIS-Home project aims at providing a full-stack, secure-by-design, and consistent software framework for improving the resilience of interconnected smart home systems. The framework enables the development of secure, privacy-aware, and accountable applications, algorithms, and services, and makes it possible to detect and dynamically react to cyberattacks and intrusion attempts or violation of user-defined policies, thus increasing control of and trust in smart home systems for the end users.

This deliverable obsoletes and replaces the deliverable D7.3 *Preliminary Business and Exploitation plan*, and provides the *Final Business and Exploitation Plan*, which paves the way to sustainable exploitation of the project results following its completion. Furthermore, this deliverable provides an exploitation strategy including: objectives and methodology; a market analysis that considers the market potential, trends and players, potential business models and scenarios; a business and exploitation plan for the SIFIS-Home framework; and the individual partners' exploitation plans and activities. The implementation of the exploitation strategy, including the business plan, aims at ensuring that the project outcomes remain viable, sustainable, and fruitful after the project has run its course.

Consistent with the objective 7 "*SIFIS-Home will actively disseminate and exploit the project results and will engage in activities devoted to standardize such results"* stated in the project proposal, SIFIS-Home will exploit the project results by presenting new commercial opportunities for vendors of security products and for developers of secure and privacy-aware Smart Home applications. This will be achieved by leveraging the influential position on the national and international markets of the industrial project partners, which include main players in the IT- and IoT-security market.

Consistent with the mission statement of SIFIS-Home, the described exploitation strategy builds on the exploitation objectives and describes a methodology that provides different ways to achieve those. The exploitation strategy provides the basis for implementing, replicating and commercializing the proposed solutions and technologies in the broadest possible context.

# Table of contents

# 1 Exploitation Strategy

This section outlines the exploitation objectives and methodology for the SIFIS-Home project. The exploitation strategy is based on the following mission statement of SIFIS-Home to provide the basis for implementing and replicating the new technologies in a broader context.

The SIFIS-Home mission is to improve the resilience of interconnected Smart Home systems, by providing a full-stack, interoperable software framework for the enforcement and management of security and safety in Smart Home systems.

SIFIS-Home provides:

- Development Application Programming Interfaces (APIs) compatible with a major commercial Internet of Things (IoT) architecture for development of certifiable, secure and privacy-aware applications.
- A resilient, fault tolerant, secure-by design software framework to handle privacy-aware data management, privacy-preserving data analysis, secure communication, system security, key management, security and safety policy management, anomaly and intrusion detection and prevention.

The underlying principle guiding the exploitation objectives and methodology is about building trust, acceptance, and confidence in the fact that it is possible, feasible and sustainable to make home automation solutions truly secure and safe to use in terms of data security and integrity as well as of system robustness and availability. Since the SIFIS-Home project is a Research and Innovation Action (RIA) project, a corresponding business and exploitation plan has been developed considering the specific characteristics of such project type: a RIA *establishes new knowledge* or *explores* a new or improved technology, product, process, service or solution (European Research Executive Agency 2023).

The exploitation strategy described here includes the exploitation objectives, methodology, Intellectual Properties (IP) and innovation management, community building and outreach roadmap. These are the foundation for the business and exploitation plan, which entails all the sections of this document, including the analysis of the smart home market, business scenarios for SIFIS-Home, the definition of key exploitable results (KERs), the specific exploitation of the SIFIS-Home framework, and the partners' individual exploitation plans and activities.

## *1.1. Exploitation Objectives*

SIFIS-Home has the following exploitation objectives:

- Objective 1: Monetize the project results and solutions and maximize their financial return
- Objective 2: Explore current and future needs of potential customers that can be addressed by

further developments in IoT security, especially through (enhanced versions of) the project results and solutions
- Objective 3: Improve the know-how and progress the state of the art in the area of IoT security
- Objective 4: Create general guidelines and a framework to guide the European IoT ecosystem towards a commonly agreed-upon development of secure IoT solutions for the benefit of the society

The adoption of the project results in various application domains further contributes to the impact of their exploitation. The following Section 1.2 explains the different ways of reaching these objectives.

## *1.2. Exploitation Methodology*

This section describes the project exploitation methodology, by explaining the different ways that will be used for reaching the exploitation objectives from Section 1.1.

The different ways of exploiting the results from SIFIS-Home, in relation to the exploitation objectives, are the following:
- Integration and usage of the developed technologies and solutions in existing and future product offering (Objective 1)
- Exploration of new business opportunities for developed technology and solutions (Objective 1)
- Lead innovation and further development based on feedback from (potential) customers of the project partners (Objective 2)
- Usage of the project know-how, results and solutions to progress research and development as well as to and support related education activities (Objective 3)
- Inclusion of technologies and solutions developed during the project in relevant standards, or development of related, self-standing standards (Objective 4)
- Submission of a follow-up Innovation Action (IA) project proposal with higher technical readiness level and industry-driven focus (Objectives 1, 2, 3 and 4)

Each of the ways is described in more detail below.

***Integration and usage of the developed technologies and solutions in product offering***

This is especially targeted at industrial partners to further improve and develop their product and service offering. More detailed exploitation plans by each partner are described in Section 6.

***Exploration of new business opportunities for developed technologies and solutions***

The technology and solutions developed in the project open up new business opportunities for project partners. These are explored by formulating business scenarios and potential new business models for commercializing the project results, as well as identifying new business opportunities related to the key results of the project. Potential business scenarios are described in Section 3, while exploitation opportunities related to each KER are described in Section 4, the business plan for the SIFIS-Home framework in provided in Section 5, and the exploitation plan of each partner is described in Section 6.

***Development as and inclusion in relevant standards of technologies and solutions developed in the***

***project***

As a far-reaching exploitation result, technologies and solutions developed in the project are being included in lightweight security standards of wide applicability and suitable for smart home applications. By being lightweight, these solutions contribute to a low energy footprint and sustainable operations and are efficient also for constrained battery-powered wireless devices. Contributing to the definition of a standard in a Standard Developing Organization (SDO) is an activity that offers a high exploitation potential for small and medium enterprises (SMEs) and large industrial partners alike, thus providing a tangible impact on society. By also contributing to and encouraging the development of open-source implementations of these standards, the efforts needed for real-life deployment are significantly reduced. The standardization activities of the project are described in detail in deliverable D7.5.

***Lead innovation and development based on feedback from (potential) customers of the project partners***

One form of exploitation is considering the feedback received from (potential) customers of the project partners. This step is likely to be facilitated by building on the focused and real-life demonstrations produced in the project. This is mostly intended to the industrial partners, as expected to leverage their existing customer connections and to continue attending various events after the project with potential future customers that can benefiting from the technologies and solutions developed in SIFIS-Home. Such events include workshops, fairs, and conventions where the project partners can present and demonstrate project results and developments of those to potential customers and receive valuable feedback.

***Usage of the project know-how, results and solutions for research, development, and education***

The project results will be exploited and used for research and development purposes, as well as for education and dissemination at large. Regarding the latter, the project results will also be used for planning the content of courses, and the learning acquired during the project and some key results will be integrated into those courses, thus effectively impacting the curricula of the students and providing a pool of top-notch talents to the industry. Smart home and IoT security are also interesting topics for thesis works as well as for academic publications, and the project results as well as future research outcomes building on those can result in valuable input to the research community and in international publications. Finally, main project outcomes will be used as base and input to forthcoming additional European and national funded projects, thus leveraging on the knowledge acquired by project partners during the execution of the project work.

***Submission of a follow-up Innovation Action (IA) project proposal with higher technical readiness level and industry-driven focus***

A follow-up IA project proposal with higher technical readiness level and industry focus is planned to be submitted in a future EU call to increase the technical readiness level of the project solutions developed in the SIFIS-Home project for more effective and broader commercial exploitation purposes. In addition, main project outcomes will be further used as base and input to other European and national funded research and innovation projects.

## *1.3. Guiding Principles for Exploitation*

Different exploitation methods described in Section 1.2 are specifically adopted by different project partners, based on their respective characteristics. Consistently, the adoption is based on the following guiding principles:

*Universities* intend to exploit project results in the form of contributions to teaching activities (both graduating and continuous professional development courses), publications, and workshops. Moreover, they intend to reuse the developed technologies for subsequent projects.

*Research Institutes* intend to exploit the project results by means of publication activities and standardization activities, their incremental reuse and follow-up developments also within subsequent projects and R&D activities, and their transfer to third-party companies as a way of improving their level of competitiveness.

*Industrial Partners* intend to exploit the project results by introducing new policies, products and solutions, and/or by integrating the newly developed technologies and solutions in their existing policies, products and/or services, and finally extending the project outcomes in other future funded research activities.

Detailed exploitation plans by each partner are presented in Section 6. The joint business and exploitation plan for the SIFIS-Home framework is presented in Section 5.

## *1.4. IP and innovation management*

The IP background of each partner was defined in the Consortium Agreement (CA) and signed by the whole SIFIS-Home consortium at the beginning of the project. The general principles for handling Knowledge and Intellectual Property Rights (IPR) within SIFIS-Home are stated below.

**Ownership**: Each participant will own the foreground it generates.

**Joint ownership**: When the foreground is generated jointly and it is impossible to determine the respective share of the work, the foreground shall be jointly owned by the participants who generated it.

**Inclusiveness, accessibility, and licensing**: The SIFIS-Home partners will avoid any proprietary software lock-in and intend to provide free and open-source reference implementations for all the necessary components. Details concerning this will be addressed in accordance with what is defined in the CA.

Software deliverables will be based on internet-standard developer environments and services for easy exploitation. All non-software deliverables of the project will be licensed as Creative Commons, with the exception of academic publications that will have to comply with the licensing terms and rights of the academic publication venue. Where applicable for media, all these deliverables will be placed also on Wikimedia Commons for easy dissemination and access.

All SIFIS-Home specifications, frameworks, data-formats, and API interfaces and specifications will be based on relevant royalty-free Internet standards, including but not limited to work by standardization bodies such as the W3C, the IETF, and ETSI.

To support the commercial exploitation of the project results, the consortium worked to capture, assess and appropriately protect the exploitable project results both at an individual partner level and at the whole consortium level. During the project, the key exploitable results (KERs) were defined and evaluated jointly by the consortium based on their degree of innovation, exploitability and potential impact. The KERs are described in Section 4.

Following the process of defining and evaluating the KERs, the SIFIS-Home Framework was analyzed in more detail as the main project result, and a specific business and exploitation plan was developed to enable its effective, commercial exploitation after the end of the project. The business and exploitation plan for the SIFIS-Home framework is presented in Section 5.

## *1.5. Community Building*

To maximize the exploitation potential and the impact of the technologies and solutions developed in the SIFIS-Home project, various community building activities were initiated since the beginning of the project. The SIFIS-Home partners engaged in several community building activities, which are described in detail below. The stakeholders and communities related to these activities were identified by the project partners as relevant ones in the application and technological areas addressed in SIFIS-Home. The community building activities and the outreach roadmap described in Section 1.6 build an open-source strategy to disseminate the project results and to attract the widest possible audience in the interest of their exploitation. Moreover, both the community building and the outreach roadmap, together with the dissemination activities described in D7.6, act as a means to increase trust among users and developers towards secure smart homes and IoT systems. This is crucial for ensuring a wide adoption and sustainable development of the developed technologies and solutions. Both activities described in Sections 1.5 and 1.6 involving potential end users aim to create a developer community to utilize the project results. These activities also increase the success of exploitation of the project results by increasing the interest of third parties to utilize the SIFIS-Home technologies and solutions. All the results of the project are accessible as open-source software available on Github.

***WebThings***

- Participation in meetings of the WebThings community.
- Direct discussions with the project leader Ben Francis (Krellian CEO), on interest about integration of SIFIS-Home security components into the WebThings framework.
- Contributed to updates and fixes for the WebThings Frameworks, both in Rust and for Arduino.
    - https://github.com/WebThingsIO/webthing-rust
    - https://github.com/WebThingsIO/webthing-arduino/pull/150

***Web of Things***

- Meeting with Ege Korkan and Cristiano Aguzzi regarding our independent wot-rust implementation, with plans to test its interoperability with node-wot.
- Reported specification problems and suggested changes via their issue trackers (e.g., https://github.com/w3c/wot-thing-description/issues/1530)

***AIxIA* (Italian Association for Artificial Intelligence)**

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

***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. RISE plans to integrate into Eclipse Californium also its implementations of the security protocols Group OSCORE and EDHOC. See https://github.com/eclipse/californium
- Following-up such an integration, the resulting enhanced Eclipse Californium implementation would be in turn considerable for the open-source implementation Leshan of the OMA standard framework Lightweight Machine-to-Machine (LwM2M), which in fact builds on Eclipse Californium and for which RISE is an official contributor.

***IETF (Internet Engineering Task Force)***

- RISE is a key contributor in the international and open standardization body IETF. This especially includes involvement in the IoT-related Working Groups "Authentication and Authorization for Constrained Environments" (ACE), "Constrained RESTful Environments" (CoRE), "Lightweight Authenticated Key Exchange" (LAKE) and “Static Context Header Compression” (SCHC). A representative from RISE serves as Chair of the Working Group "Constrained RESTful Environments" (CoRE).

- The contributions above are further enhanced and concretely instantiated by participating in and driving interoperability events involving providers of different implementations from the industry and the academia, especially but not only within the official Hackathons co-located at the main IETF meetings.

- The standardization work carried out in the IETF Working Groups mentioned above is related to and cross-pollinates with further initiatives such as:

    - Activities in the IETF Research Group "Thing-to-Thing" (T2TRG);

- Activities in the standardization bodies 3GPP and Open Mobile Alliance (OMA) as relying on IETF building blocks to build their specifications.

- Activities with other academic and industrial partners engaged in research and development of lightweight security protocols for the IoT, some of whom involved in the standardization bodies mentioned above.

- Ericsson is also a significant contributor to the IETF:
  - Global Host and Running Code Gold Sponsor
  - Active in IoT security related Working Groups, leading role in the formation of the ACE and LAKE
  - Authoring of the foundational OSCORE, EDHOC and ACE-OAuth specifications

***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. Sensative has also become a gold member of the FIWARE community.
  - https://www.fiware.org/news/fiware-ihubs-network-keeps-growing-and-maturing-with-6-new-locations/
  - https://openiotlabs.io/

- The FIWARE OiL-Hub has monthly meetings and Sensative will promote SIFIS-Home activities related to FIWARE in the community.

- Sensative has further during the project started a commercial relationship with a municipality, Herne, in Germany which was only possible by Yggio being a FIWARE NGSI compliant IoT platform. Together with Herne, Sensative and the FIWARE OiL hub will work to drive more interest in FIWARE solutions in Germany.

## *1.6. Outreach Roadmap*

This section describes the planned and executed outreach roadmap for exploitation of the technology developed in the SIFIS-Home project. The outreach roadmap forms a part of the exploitation strategy by exploring the exploitation potential with relevant stakeholders and IoT communities. Table 1 below presents the events to which the project partners participated, in order to showcase and receive feedback on the results of the project from potential customers and industrial partners.

In addition to the community building activities described in Section 1.5, the outreach activities reported in Table 1 provide further insights about the potential market interest and relevant stakeholders for the SIFIS-Home project results and activities. In order to attain the best possible impact, the events were selected based on the relevance of the target audience with respect to the areas of interest and technologies and solutions developed in the project.i. Both academic and industrial events are reported,

considering their relevance for exploitation opportunities (type of the event and audience) and the type of activity during the participation of the partners in the event.

To reach the visioned end-users of SIFIS-Home, the citizens, many of the targeted events (e.g., The BroadBand Forum) include Communications Service Providers (CSP) as participants, and thus provided an effective channel to reach the citizens indirectly. CSPs almost without exception include the residential broadband router as part of their broadband service and, e.g., F-Secure is partnering with CSPs for delivering cyber security for smart homes globally. This way the channel provides an effective mechanism for the project partners to reach also the visioned end users of the SIFIS-Home technology, the citizens.

Table 1. Events attended by the project partners.

| Event name | Event type | Event location | Event information / website link | Activity at event | Title of activity | Date(s) of activity | Target audience | Audience reached | Participating partner(s) |
|---|---|---|---|---|---|---|---|---|---|
| **Broadband World Forum** | Conference | Amsterdam, Netherlands | https://www.broadband-forum.org/meetings-and-events/broadband-world-forum-2021 | Presentation and panel discussion | CPE as a Platform for Connected Home Security | 18.-20.10. 2021 | Broadband industry and customers | Approximately 80 people from the broadband industry | FSEC |
| **Fiware Alliance** | Conference | Online | FIWARE - Open APIs for Open Minds | Presentation | Joining and giving a talk | February 2021 | FIWARE Community | >50 | SENS |
| **Broadband Forum's BASe at BREKO Fiberdays** | Conference | Wiesbaden, Germany | https://www.broadband-forum.org/meetings-and-events/base-at-breko-fiber-days | Presentation | Future Proofing Connected Home Security via Research and Industry Collaboration | 13.6.2022 | Broadband industry and customers | > 80 people from the broadband industry | FSEC |
| **International Cybersecurity Forum** | Conference | Lille, France | https://www.forum-fic.com/en/home/ | Exhibition booth | Co-Security & externally funded research projects | 7.-9.6.2022 | Cybersecurity industry and research organizations | >50 | FSEC |
| **ICC 2022 / Industry Workshop #6: "Toward AI-native 6G Networks"** | Conference | Seoul, South Korea | https://icc2022.ieee-icc.org/program/industry-presentations#IW-6 | Industry Presentation | Chairing and giving a talk | 17.05. 2022 | Industry, Research | >100 | INT |
| **6G Symposium Spring 2022** | Conference | London, UK | https://www.6gworld.com/6gsymposium-spring-2022/ | Invited Talk | Giving a talk | 23.05. 2022 | Industry, Research | >60 | INT |
| **IoT Week 2022 / Session "IoT Intelligent Connectivity and Edge Computing Research Priorities"** | Conference | Dublin, Ireland | https://iotweek.org/ | Invited Talk | Giving a talk | 20.06. 2022 | Industry, Research | >100 | INT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Internet Festival** | Conference | Pisa, Italy | https://2021.internetfestival.it/ | Workshop | Chairing and organizing workshop | 4.-8.10.2021 | Research community | >100 | CNR, MIND, LUM, POL |
| **12th Workshop on Management of Cloud and Smart City Systems (MoCS 2022)** | Workshop, Keynote speech | Online | https://sites.google.com/view/mocs2022 | Presentation | Privacy Vs Accuracy Trade-Off in Privacy Aware Face Recognition in Smart Systems; Keynote "AI at the Edge" | 30.6.2022 | Research community | 25 | CNR, INT |
| **4th International Workshop on Emerging Technologies for Authorization and Authentication, ETAA2021** | Workshop | Darmstadt, Germany | ETAA 2021 - Organization (cnr.it) | Workshop | Chairing and organizing workshop | 4.-10.2021 | Research community | 30 | CNR |
| **Neowit Tech Summit** | Conference | Oslo, Norway | https://neowit.io/ | Presentation | Joining and giving a speech | 2.6.2022 | Real Estate Owners | >20 | SENS |
| **4th International Conference on Advances in Signal Processing and Artificial Intelligence (ASPAI 2022)** | Conference | Corfu, Greece | https://aspai-conference.com/%3chttp:/sensorsportal-web.emailamp.com/ | keynote Speech | AI at the Edge | 19-21.1.2022 | Academia and industry | >30 | INT |
| **IOT Solutions World Congress & Cybersecurity Congress** | Conference | Barcelona, Spain | IOT Solutions World Congress \| 31 JANUARY- 2 FEBRUARY 2023 BARCELONA (iotsworldcongress.com) | Booth & expo | | 31.1.2023-2.2.2023 | IoT industry, academic community | | CNR, FSC, CEN, POL, DOMO, SEN |
| **SPECIES Conference** | Conference | Helsinki, Finland | https://f-secure-services.force.com/operatorportal/s/species-conference | Presentation & expo | Research collaboration presentation to partner & customer network | 20.-21.9.2022 | IoT industry, telecom operators | >100 | FSC |
| **Web of Things Online Meeting** | Seminar | Online | WoT-wot-rust-Presentation - Google Slides | Presentation | WoT-Rust Introduction | 22.9.2022 | | | LUM |
| **FISC & Kyberturvallisuuden EU-rahoitus** | Seminar | Helsinki, Finland | Tilaisuus kyberturvallisuuden EU-rahoituksesta yrityksille 12.10. \| FISC (teknologiateollisuus.fi) | Presentation | Presenting SIFIS-Home as part of FSC external research collaboration activities | 12.10.2022 | Cybersecurity industry and stakeholders in Finland | >100 | FSC |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Centria DropIn** | Seminar | Kokkola, Finland | Centria DropIn -tapahtuma houkutteli yleisökseen opiskelijoita ja yrityksiä - Centria | Booth & expo | Presenting Sifis-Home as an example of a good international cooperation in cybersecurity and smart home security | 5.-6.10.2022 | Regional companies and students | >100 | CEN |
| **Prpl Foundation Summit 2022** | Conference | Amsterdam, Netherlands | prpl Summit 2022 - prpl Foundation | Participant | | 20.10.2022 | Event for Service Providers, OEMs, Silicon Vendors, ISVs and open-source developers committed to open-source and open-APIs in support of carrier-grade gateway CPE | >150 | FSC |
| **SecTalk** | Seminar | Pietarsaari, Finland | https://www.sifis-home.eu/2022/11/29/sectalk/ | Seminar | Hosting hybrid-event | 13.12.2022 | Research, industry | 16 participants on site | CEN |
| **SecTalk** | Seminar | Online | | Presentation | Privacy-Preserving Speaker Verification and Speech Recognition | 13.12.2022 | Research, industry | 16 participants online | CNR |
| **FUI+Näringsliv - Valentine´s day business matchmaking event** | Seminar | Pietarsaari, Finland | https://campusallegro.fi/evenemang/fuinaringslivet/ | Presentation and panel discussion | Presenting Sifis-Home | 14.2.2023 | Industry | >30 | CEN |
| **Vaasa EnergyWeek 2023 industry expo** | Expo | Vaasa, Finland | https://www.energyweek.fi/ | Participant | Presenting Sifis-Home as an example of a good international cooperation in cybersecurity and smart home security | 24.3.2023 | Industry, Research | >100 | CEN |
| **Wasa Future Festival** | Expo | Vaasa, Finland | https://wasafuturefestival.fi/?page_id=374&lang=en | Participant | Presenting Sifis-Home as an example of a good international cooperation in cybersecurity and smart home security | 8.8.2023 | Companies, R&D, educational institutions | >100 | CEN |

Besides, in the remit of FIWARE OiL, Sensative attended regular Open IoT labs regular events and monthly meetings with existing partners and customers, to demonstrate the technologies and solutions developed in the SIFIS-Home project (more details are provided in Section 1.5).

# 2 Analysis of the Smart Home Market

This section describes the market analysis of the smart home market and lays a foundation for the project's business planning. This section is divided into two parts: Section 2.1 describes future market trends and players, while Section 2.2 elaborates the market potential based on the analysis.

## *2.1. Market Trends and Players*

The future of the smart home market looks very promising. The major drivers for this market are increasing awareness related to safety and security, increasing consumer need for simplicity and personalized experience, the latest geopolitical changes and the energy crisis in Europe[1], and the growing need for more cost-efficient energy consumption and energy usage optimization.

The following reflects the market analysis context and relies mostly on the recent publication[2] by the Chief Research Officer (CRO) of F-Secure, Mikko Hyppönen. His extensive career in F-Secure, together with the interaction with key professionals and worldwide renown technology developed within the organization, provides credible background and insights to the development and future trends of IoT security.

To analyze the market potential, future trends and key players in IoT security, the existing trends and development of digitalization and the Internet need to be considered. The first wave of Internet revolution took computers to the web and now we are currently experiencing the second wave of the Internet revolution, which is the revolution of IoT. During this revolution, according to Hyppönen, everything that can be taken to the Internet will be taken there, turning all capable devices into smart devices. (Hyppönen 2021, 154.)

As the revolution of IoT means, according to Hyppönen, that as all the devices that can be connected to the Internet will be connected, we will be experiencing exponential increase in the vulnerability surface, as the increase is directly linked to the increase in the adoption of network connected devices. This is also known as the Hyppönen Law, "if a device is smart, it will be vulnerable" (Hyppönen 2021, 154). It has been predicted that the rise of the IoT will create a trillion network connected devices, vastly expanding the vulnerability surface of the global digital infrastructure.

This exponential increase in the vulnerability surface of connected devices is also due to the increased connection of "dumb devices" (Hyppönen 2021, 156), meaning all possible devices that use electricity will be, according to Hyppönen, connected to the Internet even though these devices do not need smart characteristics but are connected to the Internet because of the increasing value of (user) data that these devices can collect. Manufacturers are increasingly understanding the value of data collected from these devices, and eventually the costs of connecting any device to the Internet will be low enough to make

[1] See more details at Foreign Policy's report "Europe's Worst Energy Nightmare Is Becoming Reality" at https://foreignpolicy.com/2022/07/11/europe-energy-crisis-natural-gas-russia-nord-stream-1/.
[2] Hyppönen, Mikko (2021). *Internet*. Helsinki: WSOY, ISBN 978-951-0-46441-0. Published on the 5th of October 2021.

the transformation cost-efficient. (Hyppönen 2021, 156.)

Resisting the IoT-revolution will be very difficult: it can be assumed that in the future many devices won't even function if they are not connected to the Internet (Hyppönen 2021, 157). Because of this trend, securing such devices and the IoT environment will be of utmost importance, especially in the Smart Home environments where the data is often personal and sensitive. However, the challenge is that this cannot be done through conventional cyber security means (i.e., antivirus or firewall applications) as devices are not only connected to the Internet by means that the end user can partly control and configure (e.g., a local Wi-Fi-network), but also and most likely through 5G or 6G connections. Therefore, even though there are other factors involved, a major responsibility of securing the devices will be left to the device manufacturers. In other words, the manufactures of IoT devices, which in the future means almost any device, become the key players within the IoT security field. Following this logic, eventually all enterprises will turn into software enterprises. However, as the consumers most likely do not understand the value of security in IoT, ensuring an affordable and competitive, yet profitable consumer price of these more expensive secure smart devices becomes a challenge. (Hyppönen 2021, 157–160.) This trend also highlights the need for cybersecurity awareness raising and education.

In addition to the security threats associated with the proliferated vulnerability surface of the increased number of smart devices[3] the loss of privacy becomes an increasingly imminent threat associated with the development and adoption of smart devices and environments, as often sensitive data is freely collected from the users of smart devices, especially in smart home environments. As the amount of collected data also exponentially increases when the data from various devices used by one user is combined, a multi-dimensional and more accurate profiling becomes possible (Hyppönen 2021, 165).

The executive report by Frost & Sullivan (2021, 5) *Market Opportunities in Cybersecurity* identifies the IoT as one of the main cyber risk environments led by technology transformation. Furthermore, the report states that the count of active IoT devices is expected to grow over three times from 7.6 billion in 2019 to 24.1 billion by 2030. This drastically expands the vulnerability and attack surface if cybersecurity and privacy measures and processes for IoT platforms, environments and devices are not adopted.

At the same time, according to an analysis by Fortune Business Insights (2022), the increased adoption of IoT solutions and devices boost the smart home market: "The IoT platform is one of the most significant global economic drivers for the smart home market growth. -- According to GSMA Intelligence, the IoT connections are expected to reach approximately 25 billions globally in 2025, up from 10.3 billions in 2018." Main players within the smart home market, such as Bosch, are planning to establish a firm position in the smart product's market especially for connected security and climate-control solutions to increase the user-friendly features of smart home. Therefore, the increased adoption of IoT solutions will facilitate the growth of the global smart home market during the upcoming years.

[3] Relevant mostly for IoT devices, device hijack is a type of cyber attack where the attacker takes over the complete control of the IoT device or platform (Frost & Sullivan 2021).

Current applications of universal IoT solutions include for example ABB-free@home, Google Home and Amazon Alexa. They all differ from one another in terms of scalability and connectivity. They all aim to make it easy to combine all aspects and applications inside a home to control them and add value to otherwise rather plain objects which require manual input.

Examples of players in the current market and their main features and selling points are:

**ABB-free@home**

- Light control: control the mood of the space with light control and switch it on or off individually or by groups.
- Blind control: controls shutters, blinds and curtains in groups or individually.
- Heating and cooling: remote control of heating and cooling systems.
- Door communication: see who is at the door and open the door remotely for welcomed guests.
- Safety: get alarmed via movement detectors or cameras in case, for example, burglars are detected.
- And several additional features including voice-based control.

**Google Home**

- Lighting: control connected lights and light colors.
- Climate and energy: save energy using connected thermostats, fans and air conditioners.
- Security and awareness: smart doorbells, cameras, locks and other sensors to make you feel safer at home.
- Entertainment: control smart TVs and more.
- Appliances: connect smart vacuums, ovens and other home appliances.

**Amazon Alexa**

- Lighting: control connected lights through phone or voice when paired with Alexa.
- Cameras: smart cameras that monitor activity inside and around the home.
- Televisions: using voice to open apps, changing channels and adjusting volume.
- Thermostats: controlling heating and cooling to adjust temperature when in or out of home.

Similar proposals to the solutions above deriving from the maturity of the SIFIS-Home framework include the Home Assistant and Nabu Casa.

**Home Assistant**

Home Assistant is an open-source smart home software for home automation systems. Home Assistant

is installed in a smart device, and it acts as central control system for providing home automation. There are integrations available for more than 2500 devices that can be connected to Home Assistant. Home Assistant can be accessed through a web-based user interface or by using a mobile app. There is also a subscription service available, provided by Nabu Casa.

**Nabu Casa**

Nabu Casa Inc was founded in 2018 by the founders of both Home Assistant and Home Assistant OS. Nabu Casa is a cloud service and an extension of Home Assistant. Nabu Casa is a proprietary service that offers monthly subscription plans, and also contributes with new open-source features for Home Assistant.

There are known risks and controversies regarding household appliances and the fact of connecting them to the Internet. An example of one such risk is the possibility of private conversations being listened to (Clauser 2019). Customers need a secure and transparent solution to be able to trust and confidently use the connected ecosystem, as opposed to current solutions which are mainly created by large international conglomerates that draw attention to themselves.

## *2.2. Market Potential*

Based on the background described in Section 2.1, the market potential for secure IoT platforms is expected to be significant. According to a market analysis conducted in 2016, there are nearly fifty different IoT platforms that existed at that time (Partha, 2016). The explosive growth of network connected devices and the fast development of IoT systems during recent years have only increased. However, the improvement and adoption of security measures have not followed the same development trend. IoT platforms face different concerns related to privacy and security of transmitted data, and safety and security concerns are amplified when IoT systems are built in smart homes, where they may cause physical damage and even threaten the privacy of individuals. A descriptive example of IoT security concern is their susceptibility to hostile takeover via botnet, which has been proven to be effective (Maloney, Reilly, Siegel & Falco 2019). It can be deduced that, without building trust in these devices through security solutions and means, the adoption of IoT devices can decelerate. Therefore, taking a security-by-design approach from the early manufacturing phase and all the way through deployment, operation, maintenance and decommissioning will have a high effect on the market potential of cyber secure smart home systems and smart devices.

According to the report (2022) by Grand View Research[4], the global smart home market size was valued at US $62.60 billions in 2021 and is expected to expand at a compound annual growth rate (CAGR) of 27% from 2022 to 2030. The smart home market size is forecasted to be worth US $537.01 billions by 2030. According to the report, “This growth is due to the increased focus among individuals to deploy energy-efficient devices and optimize resource utilization. The increasing importance of deploying security systems to reduce the threat of losses is significantly impacting the smart home industry growth. The introduction of advanced technologies, including security and access regulators, heating,

[4] https://www.grandviewresearch.com/industry-analysis/smart-homes-industry

ventilation, and air conditioning (HVAC) controllers, wireless technology, and entertainment controls, is anticipated to foster the market growth in the coming years." Most of these described areas fostering the strong growth of the smart home market are considered and focused on in the SIFIS-Home framework, and are therefore aligned and consistent with the strong exploitation potential and business opportunities for the project results.

As a comparison, according to a Statista[5] analysis (2021), the revenue in the smart home market is projected to reach US $115 billions in 2022. The revenue is expected to show an annual growth rate (CAGR 2022-2026) of 13.97%, resulting in a projected market volume of US $195.20 billions by 2026. Moreover, in the smart home market, the number of active households is expected to amount to 573.7 million users by 2026, and the household penetration will be 14.2% in 2022 and is expected to hit 25.0% by 2026. Therefore, there is a clear indication of a future, strong market growth for smart home systems and related technologies.

Concerning the market analysis and forecast of smart home security, technologies and solutions developed in the SIFIS-Home project, the following analysis by F-Secure about households with fixed broadband connection provides further insights. The number of households with a fixed broadband connection is estimated to reach over 1.2 billions in 2021 (World Bank 2021). By assuming a relatively conservative growth rate of approximately 4 % with a churn of 6 %, a minimum of 120 millions new consumer fixed broadband routers are taken into use annually. The total number is much larger, as things like upgrading routers approaching the end of their life cycle, replacing defective ones and replacements due to people moving, etc. are excluded from the 120 million figure above. On top of the 1.2 billion households, there are households that rely on mobile broadband on 4G and increasingly on 5G. The organic new router deployments are one channel that for example F-Secure is planning to exploit in getting Connected Home Security into the market[6]. CSPs almost without exception include the residential broadband router as part of their broadband service and F-Secure is partnering with the CSPs for delivering cyber security for smart homes globally[7]. This channel also provides an effective mechanism for the project partners to reach the envisioned end users of the SIFIS-Home technologies and solultions, i.e., the citizens. The high number of current and future households reached by F-Secure provides an extensive reach to the citizens via CSP.

Based on the market analysis provided above, the following market levels are explored to support the exploitation of the project results, solutions and technologies developed in SIFIS-Home:

*Internal market*: the exploitation is linked to the launching customers' demand, to be covered by the technology providers in the project. The participating academic partners, SMEs and large industrial partners themselves present a significant market for the SIFIS-Home results to be exploited. As an example of the potential within industrial partners, Riots currently has IoT devices in the building and home automation sectors, within over a thousand apartments. The devices could be harnessed to use the SIFIS-Home framework in order to benefit of higher security and provide a more versatile system

[5] https://www.statista.com/outlook/dmo/smart-home/worldwide
[6] For further details see Section 3.3. and Section 5 describing F-Secure's exploitation plans.
[7] Further details of F-Secure's partnerships at https://www.f-secure.com/en/partners/operators.

architecture with additional features.

*European market*: In addition to the market provided by the end-user partners, the participating commercial and academic partners will participate in onsite workshops including live demonstrations. Furthermore, the technology providers will use their own marketing strategies, relying on their existing capacities and privileged positioning (e.g., F-Secure can reach over 200 service and telecom partners[7]) for deploying SIFIS-Home results.

*Full market*: The full market roll-out will be developed considering that several technology providers as well as end-users are European (global) players. This will tackle the market within and beyond Europe.

# 3 Business Scenarios and Opportunities for SIFIS-Home

This section examines the SIFIS-Home project through the lens of the Business Model Canvas (BMC) by Osterwalder (2010) and envisions potential business scenarios to be targeted by the exploitation activities of the SIFIS-Home project. The business modelling focuses on developing products and services based on or benefitting from the maturation of the proposed SIFIS-Home framework. The business scenarios are based on the preliminary results achieved after the first half of the project. During the second half of the project, this analysis was revisited, followed by more concrete business and exploitation planning related to the KERs of the project (see Sections 4 and 5). The scenarios presented here are derived from the market analysis in Section 2, considering the forecasts and analysis of the market potential, as well as the identified trends and players within the field of IoT security and Smart Home.

## *3.1. Business Model lens for SIFIS-Home*

Figure 1 illustrates the Business Model Canvas from the perspective of the overall SIFIS-Home project, presenting several exploitation opportunities for the SIFIS-Home project as a whole, as envisioned in the first half of the project duration. The BMCs focuses on the SIFIS-Home solution comprising of 1) the SIFIS-Home framework and 2) the development tools for third-party developers. During the project, the exploitation pathways were iteratively analyzed, and concrete steps planned for business and exploitation are presented in Section 5.

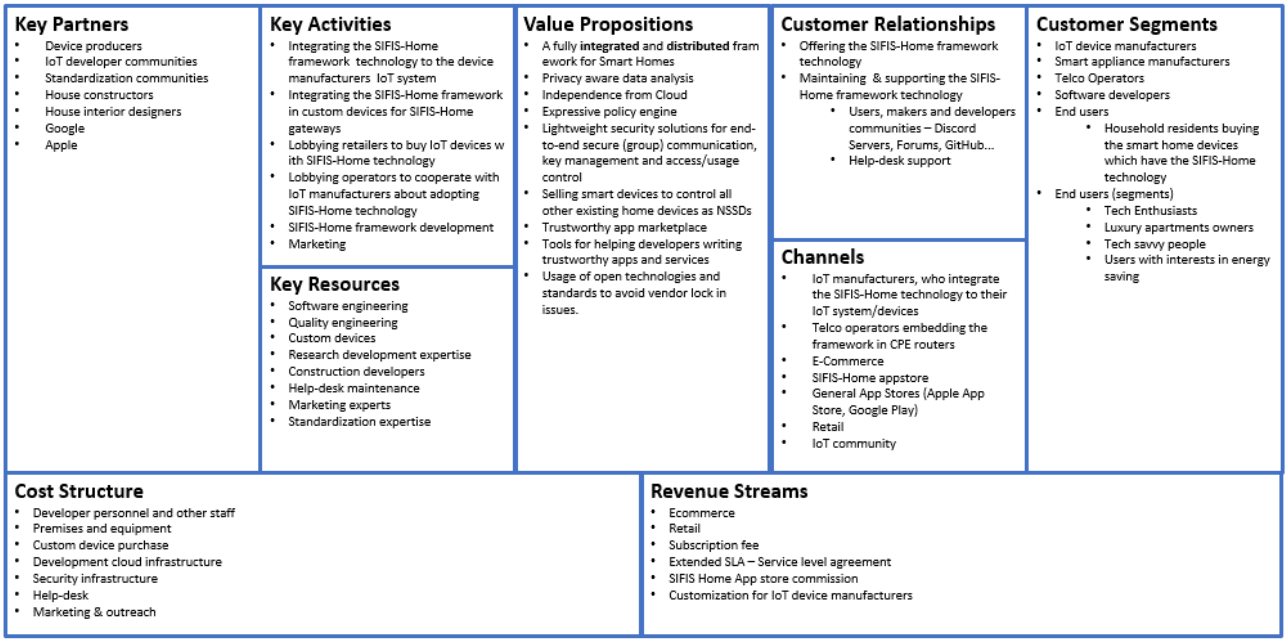


*Figure 1: Business Model Canvas for potential SIFIS-Home business exploitation*

***Customer Segments***

The customer segments cover both Business to Customers (B2C) and Business to Business (B2B). The B2C business scenario includes the direct retail to end users, which are the household residents buying smart home devices and technology. In this case, the option would be selling the devices based on the SIFIS-Home solution directly to retailers, which in turn sell those devices to the end users. In the B2B business scenario, the SIFIS-Home solution would be sold to IoT device manufacturers, smart appliance manufacturers and telco operators, which in turn would deliver their product to households through their customer channels.

Typical end users envisioned for the SIFIS-Home solution are European citizens from the following categories: technology enthusiasts with a desire of the most recent and developed technologies; tech savvy people with enough understanding of the security and privacy issues related to smart home and IoT technology; luxury household owners, and people with interest in optimizing their device usage and energy consumption in the smart home environment. Conveniency of household management is also a feature desired by a typical end-user, i.e., the citizen. Providing the SIFIS-Home technology as open source to the developer communities and third parties effectively enable the release of cost-efficient solution(s).

Especially thanks to the open-source nature of the project results, software developers are among the main exploitation targets considered in the business model. Even though there is not necessarily a direct business relationship between the software developers, there is potential for indirect business opportunities, e.g., in the form of other partnerships and collaboration.

***Customer Relationships***

Customer relationships for SIFIS-Home include offering the SIFIS-Home solution possibly together with maintenance and support services. These may be delivered through traditional help-desk support services, but also via various IT communities, including users, makers, and developer's communities, such as Discord Servers, Forums and GitHub. Customer relationships may also be upheld by providing support and updates information via companies' communications channels (e.g., press releases and social media content on recent vulnerability detections, news on common malware, security, and privacy concerns etc.), to reach the end-users easily, pervasively, and regularly.

***Channels***

The main channels to reach the customers of the SIFIS-Home solution include: IoT manufacturers that integrate the SIFIS-Home solution into their IoT systems and devices; telecommunication operators embedding the framework in the CPE routers; E-commerce; SIFIS-Home Appstore; general Appstore (Apple App Store, Google Play) and retail. Also, the IoT community can be considered as an indirect channel delivering opensource technology via software developers and other interested stakeholders.

***Value Propositions***

The core challenges that the SIFIS-Home solution aims to solve are the resilience, privacy and security

issues associated with the smart home systems and technology solutions offered today. The main value proposition that the SIFIS-Home solution offers is a fully integrated and distributed framework for smart homes. Furthermore, the SIFIS-Home solution offers privacy aware data analysis, independence from the cloud, expressive access policy definition and enforcement, lightweight security solutions for end-to-end secure (group) communication, key management, and access/usage control. In addition, the SIFIS-Home solution provides the possibility of developing and selling smart devices to control all other existing home devices as not-so-smart-devices (NSSDs), a trustworthy app marketplace, tools for helping developers writing trustworthy apps and services, and open technologies and standards to avoid vendor lock in issues.

Below, the value propositions are analyzed in more detail.

**A fully integrated and distributed framework for Smart Homes.** The architecture presented in the SIFIS-Home project addresses one of the most relevant issues in today's smart home systems: the lack of extensible interoperability. Current smart home devices are, in fact, dependent on specific brand applications and services with small possibilities for collaboration among different devices, whose control is generally always relinquished from the user.

**Privacy aware data analysis.** Privacy is a key value and becomes even more relevant when concerning data coming from people's home. As a matter of fact, homes are the place where most private activities are performed, and a huge amount of extremely sensitive data can be collected. Relying on external analysis services to perform support operations (from listening to voice command, to providing protection from physical intrusions) has the risk to entrust the service provider with full or excessive access to multimedia data collected in the home premises. The service provider might argue that they need access to such data to actually provide a service. SIFIS-Home provides a set of mechanisms to perform analytics on anonymized data, including multimedia ones. The usage of such analytics ensures that, while data are collected inside the smart home cyberperimeter, they are stored and/or sent to external services in the cloud only if they have been first anonymized. Thus, a SIFIS-Home compliant cloud service will be able to perform analysis and provide a service, without having access to privacy-sensitive information.

**Independence from the Cloud.** The reliance on cloud services, although bringing some advantages, becomes a critical weakness and a single point of failure in smart home systems when working Internet connection is needed to reach the service. Furthermore, the dependency on the cloud creates privacy issues, as the service provider might have full access to the user data. SIFIS-Home fosters a model where, thanks to the fact that the quality of services can be improved by the availability of a cloud, the system is able to remain functional also when lacking a working Internet connection. Commands and operations are processed directly within the smart home cyber-perimeter and if needed are sent in the cloud after proper anonymization. Privacy is becoming an increasingly perceived value from commercial users, and the independence from the cloud is a main enabler for more effectively building on a privacy preserving paradigm, as well as a key design choice that drovethe project activities withing its WP1.

**Expressive policy definition and enforcement.** WP3 & WP4: Comfortable and secure management of smart home environments revolves around the presence of a rule engine capable of processing and enforcing expressively defined routines and policies. Current rule engines are either hard-wired directly

by the home automation installer, thus being difficult to configure, or they lack proper mechanisms of conflict solving creating misfunctioning, or they require high computational capability to run effectively. SIFIS-Home proposes a decision engine based on the Usage Control Paradigm, which is event based, stateful and based on policies written in a markup language, which are interpreted by a dedicated engine, without hard coding in the application or service code any condition. This de-coupling allows the definition of complex policies, where conflict solving can be done at the time of policy definition. The status of the system is kept on a database-like component, thus limiting memory consumption and without the need for active processes thatmonitor conditions and events.

**Lightweight security solutions for end-to-end secure (group) communication, key management and access/usage control.** WP3: Such solutions fill existing gaps in the technology landscape applicable to the IoT, by providing end-to-end security also in group communication environments; establishment, renewal and provisioning of keying material; and fine-grained, dynamic enforcement of access/usage control also possible to pair with key provisioning.

**Selling smart devices to control other home devices as NSSDs.** WP6: This builds on the crisp separation of smart home devices in two sets: smart devices and not so smart devices (NSSD). Smart devices are those devices capable of installing third party applications, which makes them the core of each SIFIS-Home instance. Each smart device becomes, according to the SIFIS-Home architecture, responsible for one or more NSSDs, ensuring that these NSSDs can only be controlled by their responsible smart device. This element is a key aspect for security, as it can help promptly detect misbehaviors of NSSDs. This design choice could affect the future design of IoT devices, to make them compatible with new generation smart home framework like the one proposed in SIFIS-Home, including thus the possibility of updating the device software to fully support integration with the framework.

**Trustworthy app marketplace and Developer Tools.** WP2 & WP5: The trustworthy app marketplace is the service offered to developers to make their applications and services available to SIFIS-Home tenants and administrators. The marketplace proposed by SIFIS-Home also includes indications of the quality and security of applications, as a result of a compliance evaluation with respect to the SIFIS-Home framework. The SIFIS-Home marketplace, together with the developer tools provided by WP2, aim at creating a virtuous circle, where the apps developed by developers following guidelines and producing apps of good quality, without security issues, are more advertised to end users, who are instructed about safety and security risks of low-quality applications. The marketplace is a key component of the activities of WP5.

**Usage of open technologies and standards to avoid vendor lock in issues.** SIFIS-Home relies on and contributes to open standards and technologies. Through the activities of the various WPs, SIFIS-Home is increasing its engagement in open(-source) activities such as those within Fiware, W3C Web of Things (WoT) and the IETF. The usage of open-source technologies and the SIFIS-Home commitment to releasing everything as open source is important, as it avoids vendor lock-in issues. If a product or service based on SIFIS-Home becomes discontinued, the code remains available to be used and upgraded by other stakeholders interested in the technology, thus avoiding that a service or set of devices become unusable after the end of an official support.

***Revenue Streams***

The main revenue streams associated with the business model are ecommerce, retail, subscription fee,

extended SLA (service legal agreement), and commission and customization in the SIFIS-Home Appstore for IoT device manufacturers.

***Key Activities***

The key activities required for the business model are: the integration of the SIFIS-Home framework into the systems of IoT device manufacturers IoT; the integration of the SIFIS-Home framework into custom devices to act as SIFIS-Home gateways; influencing retailers to buy IoT devices that rely on the SIFIS-Home solution; influencing operators to cooperate with IoT manufacturers about adopting the SIFIS-Home framework and about considering ongoing developments in the SIFIS-Home framework, in the interest of further improvements, updates and marketing activities.

***Key Resources***

The main key resources required by the value propositions and the business model are software engineering, quality engineering, custom devices (e.g., the "SIFIScast"[8]), research development expertise, construction developers, help-desk maintenance, marketing experts and standardization expertise.

***Cost Structure***

The main cost structure includes the developer personnel and other staff, working premises and equipment, custom device purchase, development cloud infrastructure, security infrastructure, help-desk services and marketing & outreach activities.

***Key Partners***

The key partners required for the business model are device producers, IoT developer communities, standardization communities, household constructors, household interior designers and other relevant industry players.

***Additional Business Models***

While the provided BMCs represent a product related to a possible exploitation of the SIFIS-Home project as a whole, for the sake of completeness we have also extracted two additional canvases related respectively to a B2C and B2B potential products, deriving from the SIFIS-Home results (see figures 2 and 3).

The B2C product is the software framework of SIFIS-Home to be installed in smart home premises. The B2B is instead a framework to develop SIFIS-Home aware applications, together with the related marketplace. In the following, we report the two BMCs and the Strengths, Weaknesses, Opportunities,

[8] Similar to Google Chromecast, more details at: Stream Content with Chromecast (3rd Generation) - Google Store

and Threads (SWOT) analysis for these potential products (see figures 4 and 5).

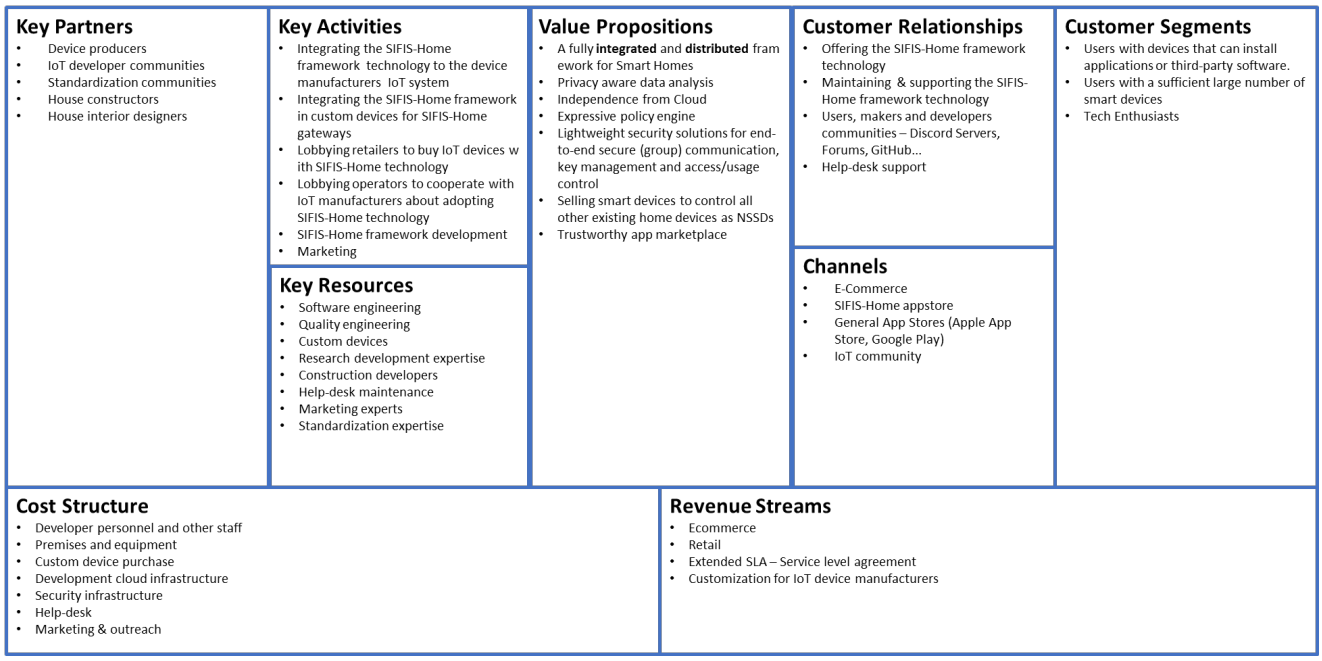


*Figure 2: Business Model Canvas for the potential B2C product from the SIFIS-Home results*

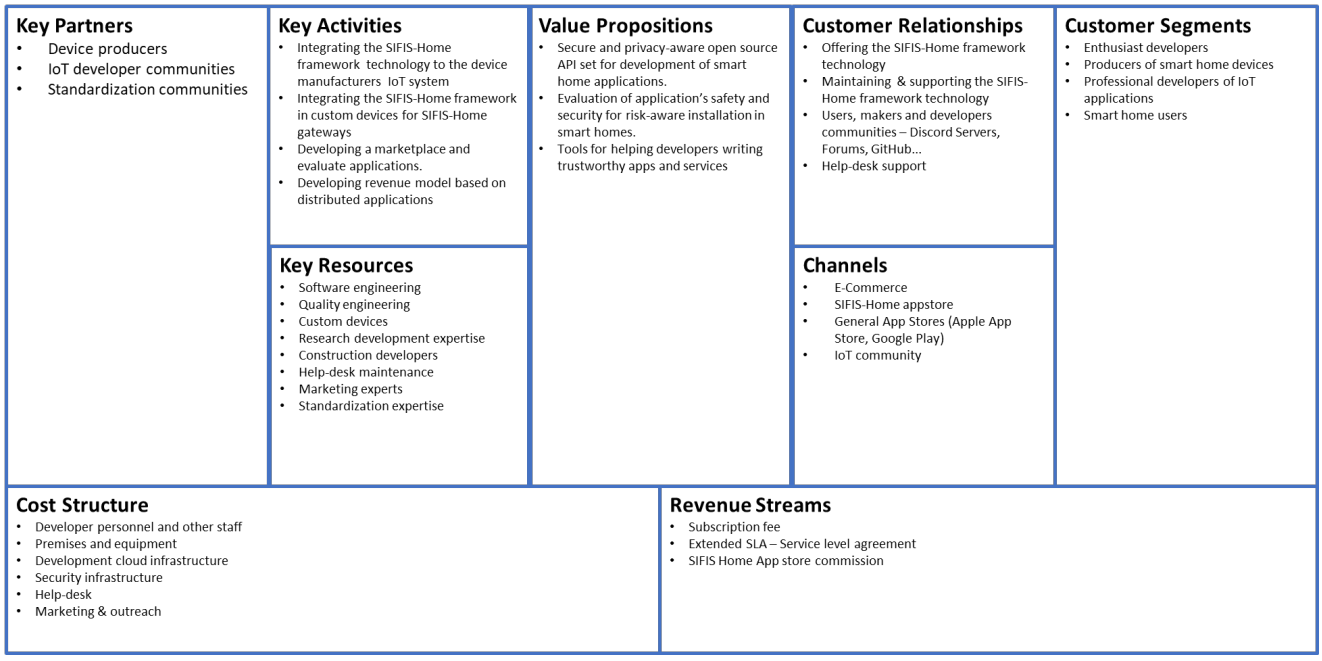


*Figure 3: Business Model Canvas for the potential B2B product from the SIFIS-Home results*


*Figure 4: SWOT Analysis for the potential B2C product*


*Figure 5: SWOT analysis for the potential B2B product*

## *3.2. Business Scenarios*

Business scenarios for the SIFIS-Home project were developed during the first half of the project and revised during the final months of the project. These focus on developing products and services coming from the maturation of the proposed SIFIS-Home framework.

***The SIFIS-Home Solution***

This section describes the potential business scenario of the SIFIS-Home solution, and presents a potential, joint exploitation activity. The business model presented in Section 3.1 refers to the exploitation potential and business opportunities of the SIFIS-Home solution as a whole. The business scenario described here provides details of the potential business landscape and market context.

The interconnected smart home is an emerging application paradigm, which is bound to have an exploding market (see further details in Section 2), involving device producers, architecture designers and application developers. The current landscape of smart home environments is highly heterogenous. While the major service providers (e.g., Amazon, Google or Mozilla) are developing advanced solutions for providing smart services to users via smart home assistants (e.g., Google Home, Amazon Alexa), there are device producers and application developers developing products to interact with the solutions in high-volume fast-paced environments, and the security and privacy aspects are generally neglected or deprioritized. This process strengthens the risk of creating an attack-prone smart home environment. As a result, the potential users have to decide if they either enjoy the functionalities of an interconnected smart home system, potentially endangering their security, privacy and safety, or refrain from becoming smart home users altogether.

In addition, the developers of smart home applications face significant challenges due to the insufficient attention to security aspects in smart home environments, as they are expected to develop applications and services for an environment rapidly changing, where new and obsolete features and functionalities co-exist.

The SIFIS-Home solution enables a secure, interoperable, full-stack IoT system for Smart Home environments. The solution aims to significantly improve the resilience of interconnected Smart Home environments, while relying on a data management approach that aims at completely privacy-preserving storage, usage and transmission of data, as completely controllable by the Smart Home user. The SIFIS-Home solution addresses the issues of lack of resilience of current Smart Home systems, by deploying an architecture which is intrinsically fault tolerant, through replication of functionalities among interconnected devices, and distributed, replicated data storage. The solution offers seamless and transparent, while still highly configurable, management of security and privacy. By doing so and as an important consequence, the solution also aims at increasing trust and acceptance among users, to speed up the wide-spread adoption of secure-by-design smart devices and smart services. This in turn increases

the Smart Home market size, especially in Europe.

Furthermore, the SIFIS-Home solution offers tools for Smart Home developers by providing secure development guidelines specific for Smart Home applications and a set of development tools integrated with the Web of Things framework to develop accountable, secure-by-construction and privacy-aware applications. As a result, these applications will exploit the SIFIS-Home solution functionalities to provide services that automatically embed security management.

The SIFIS-Home solution will offer commercial opportunities especially for EU vendors of security products and for developers of privacy-aware Smart Home applications. This applies especially to large enterprises and SMEs commercializing IoT devices and services, Smart Home products, and security solutions.

Table 3. Partner contributions within the joint exploitation of the SIFIS-Home solution

| **Partner** | **Activity within the joint exploitation of the SIFIS-Home solution** |
|---|---|
| CNR | CNR responsibilities for exploitation mix with and leverage the dissemination activities. The main exploitation result for CNR is the application of technology developed for distributed access control, intrusion detection and privacy preserving analysis in a meaningful use case. One of the three missions of CNR is, in fact, technology transfer. SIFIS-Home offers a great possibility to integrate the research solutions proposed by CNR in a real and meaningful environment. CNR then aims at raising awareness on the importance of cybersecurity in critical environments, doing outreach activities toward the general audience. To this end, CNR has organized or planned events including general audience, news and press to present the results of SIFIS-Home and raising the attention toward the topics relevant to the SIFIS-Home project. |
| POL | Politecnico di Torino exploits the SIFIS-Home solution in its five courses, which deal with the topic of IoT held in Computer and Management Engineering.<br>In the context of those courses, which involved a total of approximately 420 students, in the A.Y. 2022/2023 Politecnico di Torino planned seminars on the following topics:<br>- WebOfThings<br>- Code quality for IoT software<br>- Privacy in the Smart Home |
| CEN | Centria researches and develops the relevant technologies and the challenges and opportunities they include. Cyber security and the risks related to smart home technologies are Centria's key areas of contribution to the project. Centria's cybersecurity laboratory profits from the project by providing a safe testing environment, e.g., for anomaly detection. Centria utilizes the expertise gained in its work with the relevant stakeholders, such as education of students and staff members, innovation activities with businesses and in academic collaborations. Centria has important role as an educational institution and as an active RDI-focused collaborator in ensuring that the experiences and knowledge gained from SIFIS-Home project reaches other academic entities as well as current and future experts in the relevant fields. |
| RISE | RISE plans to assist industrial partners with its research, development and standardization expertise on lightweight security protocols, with particular reference to technologies and approaches related to the standards CoAP and OSCORE. |
| LUM | Luminem is developing an independent WoT implementation in Rust. It will provide services related to supporting implementors willing to use it for their projects as well as providing field expertise regarding implementing WoT systems.<br>Luminem will also provide formation services on the developer tools joint-developed with POL. |
| SENS | Sensative develops a horizontal IoT integration platform Yggio, which is being enhanced with vital new functionalities based on SIFIS Home technologies, like improved UX, anomaly detection, marketplace and improved alarm and log handling. We do see potential to integrate the WebOfThings connectivity standard and OSCORE E2E network security related items into Yggio and we believe that this will further improve the market potential of Yggio. |
| RIO | Riots is responsible for bringing industry expertise in the form of IoT devices and software, especially regarding intrusion detection and privacy-aware analytics. There are multiple devices developed and |

| | |
|---|---|
| | designed by Riots, and both the web-based and mobile apps are available in the building and home automation markets. |
| FSEC | F-Secure develops technology to help detect anomalies that typically occur when a vulnerable smart device gets compromised. The developed technology aims to detect network activity that is outside the baseline of a given IoT device. Such activity often has malicious intents, which is why detecting the anomaly is the first and foremost task in not only blocking and/or isolating the compromised device, but also informing the end-user about suspicious activities in the SIFIS-Home network. 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. The connections to the market can be utilized for joint exploitation. |
| DOMO | DOMO is the main author of the SIFIS-Home DHT and of the WoT compliant firmware for the IoT devices used in the project pilot. DOMO released both components as open-source software and will support implementors willing to use them in their projects. |
| ERI | ERI contributes to the joint exploitation of the SIFIS-Home solution by means of research and standardization contributions on lightweight security protocols and enablers, in particular technologies and competence related to the standards CoAP and OSCORE. |
| INT | INT provides its expertise in applying AI technology at the edge, in system level design and proof-of-concepts and demonstrators design, and implementation, testing and validation best practices. INT also supports the project dissemination and reach-out activities thanks to its participation in several standard bodies, conferences, industrial events, and workshops. |

### *Interoperating Security Solutions*

The technology landscape of the IoT is still very fragmented, and this applies especially to the Smart Home domain. Interoperability is in many cases only possible with a dedicated integration effort, unless you use products from one company, an application framework from a specific platform provider or open standards. Furthermore, devices from different manufacturers usually have their own management and operation application, commonly one app per manufacturer or type of device.

To ease interoperability between different devices in a smart home, it is of substantial value that the various units support compatible data formats and data models, as well as security and communication protocols.

A fully functional smart home needs to be able to support operations in different devices depending on yet other devices, for example fire/burglar alarms, locks, motion/heat detectors, potentially from different manufacturers need to work together without limitations on operation systems, platforms used, etc.

To apply smart protection of a home, there is a need for trustworthy communication between relevant units, and to be able to set security policies which may involve different type of appliances such as mentioned above. While there exist several general-purpose security protocols, none of those are designed to be efficient for IoT settings with, for example, battery-powered wireless embedded devices where communication overhead can be a large contribution to depletion of battery lifetime. A first step towards achieving interoperability and trustworthiness combined together is to specify building blocks providing security and communication protocols that perform well independent of device capabilities, for possible further inclusion in a comprehensive framework.

The availability of such a lightweight security framework that can be implemented and installed at manufacturing time avoids the need to integrate and patch together heterogeneous, built-in security components that are specific to particular deployments and platforms. The latter approach has several disadvantages (e.g., potential mismatch between security components in device and deployment, additional sources for bugs, difficulty to reuse in other settings, risk of poor scalability, lower operating margins, etc.).

Ideally, such a security framework should be an international standard and/or composed of international standards as its building blocks, widely available as an open-source implementation, and easy to integrate into products using state-of-the-art development best practices. These are areas where the SIFIS-Home project is making substantial contributions:

- Research and open standardization of lightweight secure communication & management protocols
- Open-source software and interoperability testing with other implementations
- Tools, guidelines, and support for secure development and certification (see Section 3.2).

As a summary, one foreseen exploitation result of the project is the ability to effectively protect smart home environments in a more interoperable, extensible, and performance- and cost-efficient way, with the help of standardized security solutions and using available code implemented during manufacture through best practices.

This exploitation achievement can also be measured in terms of the willingness of different industries and academic stakeholders to invest time and resources into this development. Furthermore, a measure of success of such an exploitation achievement is how convincing the results of this project are as perceived by others, including project partners and other industrial partners, and subsequently, customers. The lightweight security standards, which RISE and ERI progressed within the SIFIS-Home project, are being deployed by companies like ASSA ABLOY, Volvo and Electricité de France. A detailed description of the standardization activities is provided in the deliverable D7.5 “Final Standardization Report”.

***Developer Tools and Certification***

One of the key problems with the development of trustworthy IoT solution is that developers might even be well aware of the best practices to follow, but, due to ready-to-market constraints and pressing timelines, they voluntarily decide to give up on some of them in order to reduce their development-to-market cycles, thus later paying a larger price due to having to address problems found only once the product is released.

Part of the SIFIS-Home activity focuses on providing tools to automate and streamline the process often neglected by the industry, so that there are fewer reasons to not use them.

The key components to consider are:

- Simpler templating tools to start new projects with all the correct setup regarding testing, continuous integration and continuous delivery from the initial commit.
- Smarter analysis tools to focus the development effort on the parts of the code that need it the most.
- Guidelines and checklists to guide the developers and introduce them to several good practices.

The increased market focus on connected devices is bringing more companies to deal with the complexity of software where their original offerings were not used to deal with.

A large deal of products in the market show that poorly prepared teams are already delivering faulty products to the market, and consumers are starting to be more aware of the risk and wary that they have fewer means to know how trustworthy a product or a company is.

The guidelines and the tools developed by SIFIS-Home can reduce the effort required to bring to market robust solutions, and the need to prove the trustworthiness of the solutions would lead to third-party certification programs.

### *Connected Home Security*

Within the Smart Home security domain, the primary aim of a security framework is to provide cyber security and protect the household residents. This connected home security business scenario is part of a larger landscape devoted to protecting the consumers' security in the cyber domain, where the goal is to enable free and safe activities online.

Connected home security seeks to both manage the risks in the connected home and bridge the physical and cyber world around IoT for example. The risk sources can be thought to be divided into cyber and physical by looking at where the risk emerges from. A threat to the household can emerge from the physical world like someone breaking in and therefore compromising the privacy and security of the members of the household, or a risky event in the physical world like a water leak. A risk can also emerge from the cyber world with consequences in the physical world. In modern buildings and households, many things are online, such as heating, air conditioning and cameras. A cyberattack on the home IoT can result in many things ranging from leaking privacy sensitive information (like audio and video feeds) from the household to physical damage for example from a compromised heating adjustment when it is freezing outside.

In addition to risk management, connected home security bridges the cyber and physical worlds by bringing visibility to how the less visible aspects of modern households are operating and executing their tasks, and most importantly, whether everything is operating as expected or not. Often, the sense of security is strengthened and increased when people have access and visibility to the device's functions, such as anti-virus software control checkups.

Connected home security would therefore be part of a larger entity of digital security and digital wellbeing of households, which would ensure the holistic management of household security of the smart home residents.

The holistic home security and privacy portfolio would therefore include (at least) the following dimensions:

- *Family rules concept*: Protect your entire family with a single service by setting healthy boundaries for your children
- *Browsing & malware protection*: Explore the Internet, and do banking and shopping worry-free
- *Privacy protection*: Stop advertisers from tracking you and help stay anonymous online
- *Device recognition*: Visibility and management of devices in your home network
- *Smart home security*: Protect your connected devices against online threats and hacking

According to a study conducted by F-Secure in 2020[9] about consumers and their behaviors in the connected home area:

- 74% are aware of the risk of hackers gaining access to their personal data through smart home devices
- 68% are familiar with the risk of their home Wi-Fi router being used for hacking into other devices at home
- 76% feel they could easily become a victim of smart home crime
- 41% say connected home security is the number one benefit in a security solution that they are willing to pay for

Therefore, it can be deduced that the connected home security business scenario has a strong market potential based on the current consumer needs within smart home security. The results of SIFIS-Home can be integrated into the existing product offerings of connected home security (F-Secure SENSE router SDK, see further information in the FSC exploitation plan) to improve the technical features and capabilities.

### *Cyber Secure IoT Certification*

Interconnected Smart Home is an emerging application paradigm, which is bound to have an exploding market involving device producers, architecture designers and application developers. The current landscape of Smart Home environments is extremely heterogenous. In this landscape, the security aspects are generally neglected or not correctly addressed, thus making the Smart Home an attack-prone

[9] F-Secure Consumer Survey: Conducted in 11 countries (Brazil, France, Germany, Italy, Japan, Mexico, the Netherlands, Sweden, South Africa, UK, USA) to 4400 respondents (400 respondents per country) in April 2020. Link to the survey results: https://www.f-secure.com/content/dam/f-secure/en/partners/operators/resources/operator-resources_CHS-infographic.pdf.

environment, i.e., vulnerable to physical intrusions (e.g., taking over control or disrupting services) or putting the user's privacy at risk (e.g., stealing information).

Furthermore, developers of Smart Home applications also pay the expenses of insufficient attention to security aspects in Smart Home environments, and thus face significant challenges. This is further complicated by the unavoidable need for developed applications and services to address an environment which is rapidly evolving and fragmented, where new and obsolete features and functionalities coexist.

To ease the challenges of fragmented development landscape and the cyber security risks associated with the IoT and smart home environments, a potential business scenario would be introducing a certification of cyber secure IoT or security-by-design smart home environments. The business scenario would therefore comprise the introduction of cyber secure IoT device certification, where the SIFIS-Home framework would include a demand for Manufacturer Usage Description (MUD) for devices developed by manufacturers to receive the certification label of cyber secure IoT devices. This would be only one requirement on top of more traditional ones such as vulnerability management and software or firmware update process over the lifecycle of the IoT device. Further details and references regarding the MUD concept are provided in the deliverable D4.2.

Through the manufacturer relying on MUD, an increased level of security can be provided by knowing the manufacturer intended behavior when monitoring and verifying actual observed behavior of the IoT device. This "cyber safe to use" certification label would also add to increasing awareness among consumers of cyber security risks associated with Smart Home and IoT devices and building trust to the security-by-design technology.

In other words, the business scenario is that cyber security actors could provide new market opportunities through certification of cyber secure or secure-by-design IoT devices and smart home environments. The certification logic would follow a similar model used in broadband routers: defined mandatory and optional security requirements on routing devices[10]. Ideally, the actors providing the "cyber safe to use" certification, would be independent entities, such as research institutes. Enterprises would be engaged in the verification and compliance revision, which can be monetized. As a result, manufacturers would receive higher value for their cyber secure products with security labels and certification.

A study conducted by F-Secure in 2020[11] about consumers and their behaviors in the connected home area confirm the potential of this business scenario, by describing consumer needs within the Smart Home area as follows:

- Consumers do not trust smart device manufacturers: 80% think that manufacturers are not doing enough to ensure online security and privacy of smart home devices

[10] For further details, please see: BSI TR-03148:Secure Broadband Router (bund.de).
[11] F-Secure Consumer Survey: Conducted in 11 countries (Brazil, France, Germany, Italy, Japan, Mexico, the Netherlands, Sweden, South Africa, UK, USA) to 4400 respondents (400 respondents per country) in April 2020. Link to the survey results: https://www.f-secure.com/content/dam/f-secure/en/partners/operators/resources/operator-resources_CHS-infographic.pdf.

- Consumers crave simplicity in the complex environment they live in, and they want to purchase security from a reliable source: 60% prefer to buy connected home security service from their mobile, cable or Internet Service Provider

Therefore, the cyber secure IoT certification would offer a feasible business scenario and be complemented by the SIFIS-Home project consortium having competitive advantage, F-Secure being the leading cybersecurity provider through operators in the consumer market. Furthermore, similar trends and research towards cyber security certification have evolved during recent years[12], confirming the analyzed business potential within the field and being an emergent area creating new market opportunities in the future.

### *3.3.6 Smart Home Business Consulting Services*

The SIFIS-Home project focuses on creating a Secure Interoperable Full-Stack IoT solution for Smart Home environments. As a result, there is a substantial number of solved problems and implemented solutions in the Smart Home scenario. All the public deliverables of the project will be open source, i.e., anyone can utilize the results. However, the result will be a huge piece of software and information that will require knowledge, time, and commitment to be fully utilized.

Meanwhile, device manufacturers are ramping up IoT development programs to connect home appliances and various other devices to the Internet. In many cases, this requires learning new skills and gathering new knowledge. Traditional home appliance manufacturing requires industrial design, hardware skill, and in some cases embedded software skills - but the things related, e.g., to cloud computing, device interoperability, connectivity between devices, SaaS business models, UI experience and mobile applications are uncharted territory for most of the established companies in the scene.

The discussion regarding business models for open-source software has been there as long as there have been open-source projects available. Regarding SIFIS-Home, there is clearly business space for professional services around the SIFIS-Home results, including the following ones:

- Selling technical support and consulting on how to build Smart Home devices
- Selling developer kits that can be used to kickstart Smart Home device manufacturing
- Utilizing Software as a service business model, providing parts of the SIFIS-Home architecture as a service, so that customers can focus on parts that are most useful for their business scenarios
- Various advertising scenarios that can be added to platform

[12] EU Horizon 2020 funded SCOTT-project (Secure Connected Trustable Things) researched similar topic of privacy labeling (https://scottproject.eu/) and as part of Horizon 2020 ARMOUR-project cyber security of certification and labelling of IoT devices was explored (https://www.researchgate.net/profile/Sara-Nieves-Matheu-Garcia/publication/327099163_Risk-based_Automated_Assessment_and_Testing_for_the_Cybersecurity_Certification_and_Labelling_of_IoT_Devices/links/5be4197a92851c6b27af571a/Risk-based-Automated-Assessment-and-Testing-for-the-Cybersecurity-Certification-and-Labelling-of-IoT-Devices.pdf).

# 4 Key Exploitable Results

The consortium has discussed and evaluated the results of SIFIS-Home during the project, Key Exploitable Results (KERs) were identified, and related exploitation opportunities discussed. These KERs were identified and evaluated based on their degree of innovation, exploitability and impact – three qualities of a KER also used by the Horizon Results Booster platform.

The following KERs were identified:

- SIFIS-Home Framework
- Developer guidelines
- SIFIS-Home Marketplace
- SIFIS-Home AUD
- SIFIS-Home DHT
- Privacy Dashboard
- Analytics Toolbox
- wot-rust

In the rest of this section, the KERs are described, starting from the SIFIS-Home Framework as the main result of the project, and continuing with other KERs which contribute to the framework and offer significant exploitation opportunities on their own. A business and exploitation plan for the main project result, the SIFIS-Home framework, is introduced in Section 5.

***SIFIS-Home Framework***

The SIFIS-Home framework builds on a new paradigm that emphasizes openness and cloud-independence, as it is fault tolerant and ensures resilience even when Internet access is not available. The architecture presented in the SIFIS-Home project also addresses one of the most relevant issues in today's smart home systems: the lack of interoperability. Current smart home devices are, in fact, dependent on specific brand applications and services with small possibilities for collaborative interaction among different devices, whose control is generally always relinquished from the user.

**Novelty.** The SIFIS-Home framework implements a novel paradigm for the management of security and safety in Smart Home environments. Having a fully distributed solution provides fault tolerance and allows the Smart Home functionalities to be provided without relying on a cloud infrastructure.

**Exploitability.** The exploitability of the SIFIS-Home framework is extremely high. Although it is the result of a Research and Innovation Action, several business models and scenarios have already been identified, where to develop products coming from (improved versions of) the framework (see Section 3). The architecture can also be extended and adapted to other environments related to the IoT. The open-source nature of the results support a wider and more effective exploitation.

**Impact.** The SIFIS-Home framework will be a leading global framework for giving developers and Smart Home device vendors easy and open access to resilient, privacy-aware and cloud-independent Smart Home technology. The impact of the SIFIS-Home framework is expected to be very relevant. In

fact, a subset of the implemented SIFIS-Home functionalities has been transferred into a commercial product by DOMO. SEN is also commercially exploiting parts of the framework and the adaptation of the Yggio platform for its integration with the SIFIS-Home DHT. Also, SIFIS-Home has had a direct impact on the W3C WoT community, where the model to classify risks associated with devices and their functionalities has been proposed and implemented. Furthermore, maturation activities on the SIFIS-Home framework have been proposed as activities of new research projects, which got funded at a national level, by Italian government. The projects are part of the prestigious PRIN (Progetti di Rilevante Interesse Nazionale) program.

***Developer guidelines***

A series of guidelines ha been derived from software engineering concepts, organized into precise workflows, and supported by tools that developers are strongly encouraged to follow in order to enhance the security and quality of IoT software running in a Smart Home environment.

**Novelty.** The guidelines contain well-known concepts and techniques that, when merged together, provide a significant degree of innovation. In fact, the developer is also supported by tools during the creation, testing, and deployment of their IoT source code.

**Exploitability.** The exploitability of the Developer Guidelines is extremely high because they can be applied to any project. The open-source nature of the result supports exploitation.

**Impact.** When developers use the guidelines, the quality of the code produced is higher because guidelines and tools force the developer to take into account tasks that are usually skipped or overlooked. As the application area of the guidelines is broad and they are made available as open source, the guidelines have the potential to be of high impact in the developer community.

***SIFIS-Home Marketplace***

The SIFIS-Home marketplace focuses on IoT applications, and makes it possible to efficiently connect different systems to each other. The aim is to become the Android marketplace for the IoT.

**Novelty.** The integration of a marketplace within a horizontal, off-the-shelf ready IoT platform like Yggio is very unique in the market. This novel concept has the opportunity to fundamentally alter the way Yggio users connect, collaborate, and utilize modern IoT technologies.

**Exploitability.** With a marketplace integrated into the Yggio IoT platform, Yggio users gain the flexibility to scale their IoT solutions rapidly and bring new services to the market, including not only those developed directly by Sensative, but also by other parties, possibly in concert with Sensative. Users can add new functionalities, devices, or services as their requirements evolve, without the need for extensive development work in the Yggio core software. This adaptability is a game-changer for Sensative, which aims to stay competitive and agile in a dynamic market.

**Impact.** By enabling a dynamic, interactive ecosystem of IoT developers and vendors, the SIFIS-Home marketplace will stimulate innovation in the IoT space and drive increased revenue for Sensative. Developers should be incentivized to create and share cutting-edge applications and services, fostering a competitive environment where new ideas flourish. This dynamic atmosphere of innovation ensures that Yggio users can continuously leverage the latest advancements in IoT technology.

### *SIFIS-Home AUD*

SIFIS-Home Aggregated Usage Description (AUD) aims to describe network behavior based on traffic observed in the network it is running on. With the help of non-intrusive means of continuous network monitoring, AUD aims to detect harmful anomalies from benign deviations in typical network traffic patterns.

**Novelty.** By definition, an anomaly is a behavior that deviates from a behavior considered to be normal. In order for a networked system to be able to detect anomalies there must be an understanding of what a normal and expected network behavior is. However, defining normal network traffic and patterns is challenging in the ever-growing IoT field filled with diverse devices communicating to various ecosystems. Standards for describing network activity of devices do exist (e.g., Manufacturer Usage Description, MUD, RFC 8520), but have so far not been adopted in consumer-oriented network environments. Possibly, this is because both network components (i.e., routers, firewalls) and target IoT-devices are required to support the technology to benefit from it.

Aggregated Usage Description (AUD) is a novel technology that aims to describe network behavior based on traffic witnessed on the network it is running on. Contrary to MUD, which involves both IoT device vendors and network hardware developers, AUD operates solely on network hardware and does not require input from IoT vendors. With the help of non-intrusive means of continuous network monitoring, AUD aims to detect harmful anomalies from benign deviations in typical network traffic patterns. This creates an effortless additional layer of network security, particularly for IoT devices that lack security features due to, e.g., end-of-life status or manufacturing cost.

**Exploitability.** AUD offers multiple exploitation opportunities as it can be integrated and deployed in a current container and for several types of routers. AUD will be integrated into F-Secure's product offering. F-Secure Sense Connected Home Security protects every single connected device in a home against cyber threats. Sense protection functionalities are embedded in Service Provider Wi-Fi routers or home gate-ways. SIFIS-Home AUD is a critical new component to be integrated in the F-Secure Sense product. The open-source nature of the result supports effective exploitation.

**Impact.** AUD complements alternative solutions and differentiates from the competition.

### *SIFIS-Home DHT*

The SIFIS-Home DHT is a novel and completely distributed solution that allows applications to easily exchange messages using a pub/sub pattern. The SIFIS-Home DHT does not rely on having a centralized message broker in the network, such as in the case of the MQTT publish-subscribe protocol, that also represents a SPOF for the system. Conversely, with the SIFIS-Home DHT all nodes collaborate to provide the pub/sub infrastructure. In case one of the nodes is removed from the network or experiences a failure, the pub/sub infrastructure provided by the DHT is still operational, and no data losses occur since the messages are stored on multiple nodes. The DHT has also a built-in mechanism to handle possible data conflicts that can arise when a network partition occurs or if nodes composing the DHT dynamically leave or join the network. In detail, it is always assured that only the last published version of a certain message is maintained and provided to the pub/sub applications. The DHT provides automatic node discovery also. In detail, whenever a new DHT node enters into the network, it is able to discover other DHT nodes and immediately start exchanging messages with them. This significantly simplifies the deployment of the solution since applications should not be provided with the addresses

of centralized brokers or bootstrap nodes.

To summarize, the SIFIS-Home DHT can overcome the limitations of other pub/sub solutions such as MQTT as it does not rely on a centralized broker, allows for automatic mutual application discovery, pub/sub communication, and data conflict management.

**Novelty.** The market is currently missing a publish-subscribe solution that is i) completely decentralized, ii) has no SPOF, iii) provides automatic data conflicts management and a distributed storage of messages. The SIFIS-Home DHT is a novel solution that fills this gap in the market.

**Exploitability.** The SIFIS-Home DHT has been run and tested using amd64, armv8 and armv7 machines. Also, amd64/armv8 docker images are available in the SIFIS-Home Github for usage by the community. The SIFIS-Home DHT can be used in a number of different scenarios, such as smart home and smart cities, network devices, connected cars, etc. In general, it should be considered for usage in all the application scenarios where there are devices/applications that need automatic discovery, pub/sub communication and an easy way to store messages/information. DOMO is currently using the SIFIS-Home DHT to exchange messages between its WiFi Gateways. Furthermore, future exploitation opportunities for other SIFIS-Home partners, such as Sensative and Riots, have been identified. For instance, based on SIFIS-Home DHT, Sensative can build a distributed network on top of Yggio.

**Impact.** The SIFIS-Home DHT is an open source, free to use solution that solves a number of issues that typically arise while developing IoT applications and, in general, distributed applications. We believe that, in the future, it could be used by a number of companies/developers working in the IoT field.

***Privacy Dashboard***

The user of the Privacy Dashboard can exercise their right to privacy according to GDPR obligations. The Privacy Dashboard allows the user to express and later revoke consent on how personal data is handled. This is made convenient for the user by using automatization, thus not requiring the user to remember where consent has been given.

**Novelty.** Although, following the introduction of GDPR, a number of services and websites already include functionalities to set up privacy preferences with a certain level of granularity, to the best of our knowledge a framework that constantly informs the user about their privacy preferences and allows to revoke all the external access right at once is something innovative.

**Exploitability.** The exploitability of this framework is pretty high. Although it has been designed specifically for SIFIS-Home, it can easily be extended and adapted to other environments, such as public administration services and applications. From the project partners, F-Secure identified exploitation opportunities as an addition to F-Secure's holistic cyber security product offering and as a competition for current “delete me” solutions in the market. The open-source nature of the result supports exploitation.

**Impact.** The potential impact of the privacy dashboard is very high as the relevance of data privacy and the need of tools to easily handle it is continuously growing. As a matter of fact, a maturation of the privacy dashboard has already been proposed in a national project (PRIN), co-lead by POL and CNR, which has been approved for funding.

***Analytics Toolbox***

The Analytics Toolbox provides a set of tools to analyze network traffic and detect anomalies. This is especially important when there are large data streams interrupting the operations of networks and applications are not acceptable.

**Novelty.** The Analytics Toolbox exploits a set of analytics based on machine learning, deep learning and statistical analysis. Differently from typical intrusion detection systems (i.e. antivirus software), which rely on pre-existent knowledge of malicious signatures to identify malicious behaviors, the mechanisms used in the analytics toolbox are able to detect zero day attacks and other unknown threats, as the identification is based on a white list approach, looking for anomalies. Moreover, the analytics toolbox sports a set of multimedia-based analytics, trained to identify physical dangerous situations, exploiting cutting edge research mechanisms which are not off-the-shelf yet.

**Exploitability.** The Analytics Toolbox is extensible by construction, thus allowing the easy integration of new analytics. Its exploitation in environments different from the smart home settings, might require re-training or fine tuning of current classifiers. The open-source nature of the result supports exploitation.

**Impact.** The Analytics Toolbox has been impactful, as the research done to implement the proposed analytics has resulted in a consistent number of academic publications. Furthermore, the technologies of the Analytics Toolbox are being extended and adapted  environments different from the smart home settings, which creates opportunities for targeting a larger number of use cases and applications..

***wot-rust***

Wot-rust is a from-scratch, Rust implementation of the following Web of Things standards: 1) Thing Description 1.1, 2) Profile (http SSE), 3) Protocol Bindings (http, coap, mqtt) with additional components being developed on top.

The main implementation of the full WoT stack is node-wot, with the WebThings community offering multiple implementations of some parts of the pre-1.1 standards (e.g., the webthings-arduino implementation that DOMO has used as base for the firmware of their actuators).

The Rust implementation aims to be modular enough to target both the embedded space, as the namib-project already showcased, and the desktop/server space without reimplementing it. This would eventually make it possible to verify the main logic and behavior of firmwares on non-embedded system (e.g., Linux) and to compile the same source code for embedded and even bare-metal targets, such as `esp32-c3 leveraging the Rust ecosystem.

**Novelty.** wot-rust is the first complete implementation of most WoT components in Rust, and it is already implementing "at risk" elements of the specification. In W3C jargon, an element of the specification is labeled as "at risk" if it is not supported by at least 2 implementations, which are required to preserve the element in the specification.

**Exploitability.** The implementation wot-rust is modular to ensure that developers can use only what they need. Since the WoT specification covers most/all the aspects of an IoT platform, and since we already had third parties that were satisfactorily using it, it is reasonable to assume that it will keep being used even more in the future. Since it is written in Rust, it is easy to embed it in C, C++, Python and Java with minimum effort and in typescript/javascript with a little more work, as the WASM/WASI

targets are still being refined. The open-source nature of the result supports exploitation. Sensative and Riots see significant exploitation potential in wot-rust for their businesses.

**Impact.** The implementation experience already brought fixes and changes to the thing description specification and validated the wot-profile for the Server Sent Events by interoperating with the related Krellian's implementation. Wot-rust has the potential to revolutionize the IoT industry, filling the gap on how devices should be interfaced and connected to each other.

# 5 Business and Exploitation Plan for the SIFIS-Home Framework

This section discusses the business and exploitation plan for the main result of the project, i.e., the SIFIS-Home framework. The following includes an overall description on how the viability of the framework is ensured after the project finishes, an analysis of go-to-market strategies including the positioning of the SIFIS-Home project, and a related business plan to monetize the framework. This business and exploitation plan was finalized towards the end of the project to pave the way for the SIFIS-Home framework to enter into the smart home market. The business plan builds on the market analysis in Section 2, the business scenarios in Section 3 and the KERs in Section 4.

## *5.1. Ensuring the viability of the SIFIS-Home framework*

The SIFIS-Home framework is the main result of the project and ensuring the viability of the framework after the project finishes is at the core of this exploitation plan. In the following, the exploitation plans and activities ensuring the viability of the SIFIS-Home framework are discussed.

Following the exploitation strategy presented in Section 1, the SIFIS-Home framework is exploited in several ways, as explained below.

- The project results are made available as open source on GitHub and they are marketed through the project website, social media channels and publications (see D7.4 Final Dissemination report), as well as by reaching out potential stakeholders as part of community building activities (see Section 1.5 “Community Building”) and by participating in industrial and academic events (see Section 1.6 “Outreach Roadmap”).
- The developed technologies that are part of the framework are used in the existing product offering of the industrial partners of the project. In addition, new services are created, such as wot-rust consulting of LUM. These are described in detail in section 6 Partners’ Exploitation Plans and Activities and Section 4 “Key Exploitable Results”.
- The technology developed in the project is included in relevant standards. One of the related exploitation results is that the lightweight security standards, which RISE and ERI progressed within the SIFIS-Home project, are being deployed by companies like ASSA ABLOY, Volvo and Electricité de France. The detailed description of the standardization activities is in the deliverable D7.5 “Final Standardization Report”.
- New knowledge created in the project has been and will be used in research and teaching by the academic partners. This is described in detail in Section 6 Partners’ Exploitation Plans and Activities.
- A follow-up Innovation Action (IA) project proposal will be submitted with higher technical readiness level and industry driven focus in Horizon Europe Cluster 3 in 2023. Furthermore, two follow-up research projects proposed by CNR and POL have been funded by the Italian Government. The projects are part of the prestigious PRIN (Progetti di Rilevante Interesse Nazionale) program, and they aim at exploiting and maturating core elements derived from the SIFIS-Home project, such as the evaluation of application risks and the Privacy Dashboard.
- New business opportunities for developed technology and solutions have been explored during the project (see section 3 Business Scenarios). This includes the development of DOMO, which is a spin off company of CNR founded during the project. DOMO is commercializing a software framework inspired by the principles of the SIFIS-Home architecture.

Among the sustainability actions undertaken by the consortium, the SIFIS-Home framework is being

pushed into the work of the recently started 40 M€ EU-funded KDT projects called ISOLDE (isolde-project.eu), where INT has a driving role being WP leader and a provider of key technology components. One of the use cases of ISOLDE is in fact focusing on smart and secure homes, and INT has proposed to the ISOLDE consortium to base part of the work in that use case on the SIFIS-Home framework. That will guarantee a continuous, long-term exploitation of one of the main project results, the SIFIS-Home Framework, into other projects, which will allow the continuation of the development of the framework outside of the SIFIS-Home consortium.

## *5.2. Positioning*

In addition to the exploitation plans and activities described in Section 5.1, an analysis of go-to-market strategies was made to guide the joint plan for commercial exploitation of the framework. Based on the analysis, a positioning was chosen for SIFIS-Home framework to enable the realization of the following vision:

*The SIFIS-Home framework will be a leading global framework that gives developers and smart home device vendors easy and open access to resilient, privacy-aware and cloud-independent smart home technology.*

Figure 6 introduces a Smart-Home Framework Quadrant (SHFQ), comprising SIFIS-Home framework and other relevant examples. The quadrant is inspired by the Gartner Magic Quadrant (GMQ) method. We developed the SHFQ to position the SIFIS-Home framework in the global market of Smart Home solutions. Unlike in the GMQ, the top-right corner in the quadrant is not necessarily the most attractive position. The purpose of the SHFQ is to study and cluster go-to-market strategies within XY-axis that have shown business results.

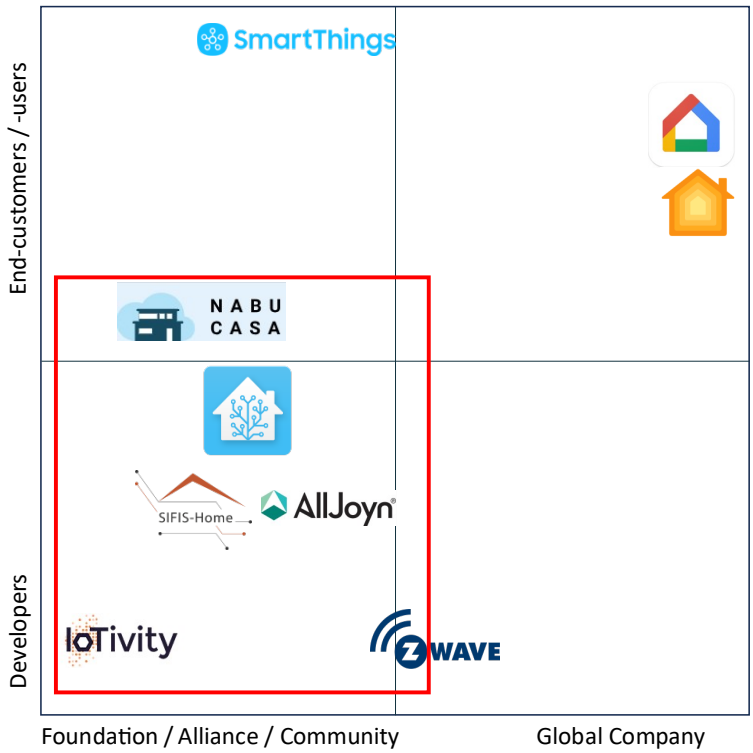


*Figure 6: Positioning of SIFIS-Home framework within Smart-Home Framework Quadrant*

The GMQ rates vendors according to two criteria: completeness of vision (X-axis) and ability to execute (Y-axis). The SHFQ does not rate go-to-market strategies. The X-axis presents two finance options. Foundations, alliances and communities are presented on the left-hand side of the X-axis, while global companies are presented on the right-hand side of the X-axis. The Y-axis presents the parts of the two-sided market that has two distinct user groups. Developers (i.e., developer community) are presented at the bottom of the Y-axis and end-users (i.e., either consumers or businesses) are presented at the top of the Y-axis.

We studied financing and go-to-market strategies of eight solutions similar to the SIFIS-Home framework, namely IoTivity, AllJoyn, HomeKit, Google Home, SmartThings, Z-Wave, Home Assistant and Nabu Casa. Our goal was to learn from cases that have been successful long-term.

**IoTivity** is an open-source framework developed by the Open Connectivity Foundation (OCF). It provides a standardized approach to enable secure and interoperable communication between IoT devices. IoTivity focuses on device discovery, data sharing, and control, ensuring security through authentication and encryption mechanisms. The IoTivity project is sponsored by the Open Connectivity Foundation (OCF) and primarily targets developers.

**AllJoyn** is an open-source framework originally developed by the AllSeen Alliance. It aims to facilitate seamless interoperability among IoT devices, allowing them to communicate and interact regardless of the underlying hardware or communication protocols. AllJoyn includes security features such as access control and encryption to protect data and ensure privacy. Qualcomm promoted the AllJoyn technology in its early stage. AllSeen Alliance sponsored the AllJoyn Project, and the Open Connectivity Foundation took over the sponsorship in 2016. AllJoyn targets primarily developers and leverages the companies of the foundation.

**HomeKit** is a framework developed by Apple for smart home devices. It provides a unified platform for device communication, control, and automation within the Apple ecosystem. HomeKit emphasizes security by requiring strict certification for device manufacturers and utilizing end-to-end encryption and authentication to protect user data. Apple owns and sponsors the HomeKit development. HomeKit works with Apple devices and leverages the existing market of Apple customers. However, Apple is currently working with Samsung, Amazon, and Google to create an open standard for smart home automation called Matter. The main goal of Matter is to achieve interoperability among smart home devices and Internet of things (IoT) platforms from different providers.

**Google Home** refers to a family of smart speakers and smart displays developed by Google. Google Home is tightly integrated with Google Assistant, which is Google's AI-powered virtual assistant. Google primarily targets end-customers in the smart home market. Google Assistant has a developer ecosystem that includes third-party developers and a growing number of third-party applications and actions.

**SmartThings** is a platform and framework currently developed by Samsung for smart home automation. It supports a wide range of devices and provides a hub to connect and control them. SmartThings emphasizes interoperability, enabling users to integrate devices from different manufacturers. It includes security features such as authentication, data encryption, and user access controls. Interestingly, SmartThings was originally developed by a set of individual developers that promoted their first prototype in a Kickstarter campaign. The target customers got excited about the prototype and the crowdfunding campaign was very successful. After a series of investment rounds, Samsung finally acquired SmartThings.

**Z-Wave** is a wireless communication protocol and framework designed specifically for smart home devices. It focuses on interoperability and reliability, allowing devices from different manufacturers to communicate seamlessly. Z-Wave employs AES encryption for secure communication and provides mechanisms for secure device pairing and network key management. The Z-Wave protocol was originally developed by the Danish company Zensys. Later on, five companies, including Danfoss, Ingersoll-Rand and Leviton Manufacturing, adopted Z-Wave and formed the Z-Wave Alliance. Z-Wave is primarily targeted at developers.

**Home Assistant** is an open-source home automation platform that allows users to control and automate various smart devices within their homes. Home Assistant is primarily a software platform rather than a business entity, but it has a significant presence in the smart home ecosystem. Home Assistant was initially created by Paulus Schoutsen in 2013 as a personal project. It gained popularity in the open-source community and among smart home enthusiasts. The development of Home Assistant has been primarily community-driven, with contributions from volunteers and the open-source community. Related to an alliance or foundation, financing is powered by the target market that are smart home enthusiasts and DIYers who wanted to have a high degree of control and customization over their smart home setups.

**Nabu Casa** was created by the founder of Home Assistant, Paulus Schoutsen, to provide a cloud-based subscription service that enhances the Home Assistant experience. Nabu Casa was introduced as a way to support the ongoing development and maintenance of Home Assistant. Nabu Casa targets Home Assistant enthusiasts.

As illustrated in Figure 6, we may find three main positions in Smart-Home Framework Quadrant. The positions are top-left, top-right and bottom left. analysis of the six cases above suggests two main categories for long-term go-to-market strategy that are top-right box and bottom-left box in Figure 6. The bottom-left is the chosen option for the long-term go-to-market strategy of SIFIS-Home framework. The SIFIS-Home framework will be targeted at the developer communities as it is the main industry practice (see Figure 6). An alliance is a long-term means to sponsor SIFIS-Home framework. The short- and mid-term plan is to finance the work in Horizon Europe and KDT JU projects. Our aim is to invite the partners of these projects and involve them in the alliance.

## *5.3. Monetizing the SIFIS-Home framework*

This section presents the business plan and a quantified monetizing model for the SIFIS-Home framework, building on the positioning analysis described in Section 5.3 and on the analysis of the smart home market and market potential in Section 2.

The following considers a lean canvas approach (see Figure 7), which – compared to a BMC – structures business planning to be focused on solving a customer's problem, instead of centered around a specific product. Furthermore, this lean business planning approach enables adjustments when the model is implemented, making it better suited to serve the needs of a lean start-up than a traditional business plan.

The SIFIS-Home framework offers many types of business opportunities, which are discussed in

Section 3 Business Scenarios. For this business plan, as related to the consortium model introduced in Section 5.1, we have taken an approach where the SIFIS-Home framework is the "Play Store" for smart homes and allows third-party developers to develop applications and store them on the platform. For a developer developing IoT applications, such as a new light manager application, this SIFIS-Home solution offers ways of controlling what the application is going to do, improving the privacy and security aspects of the application.

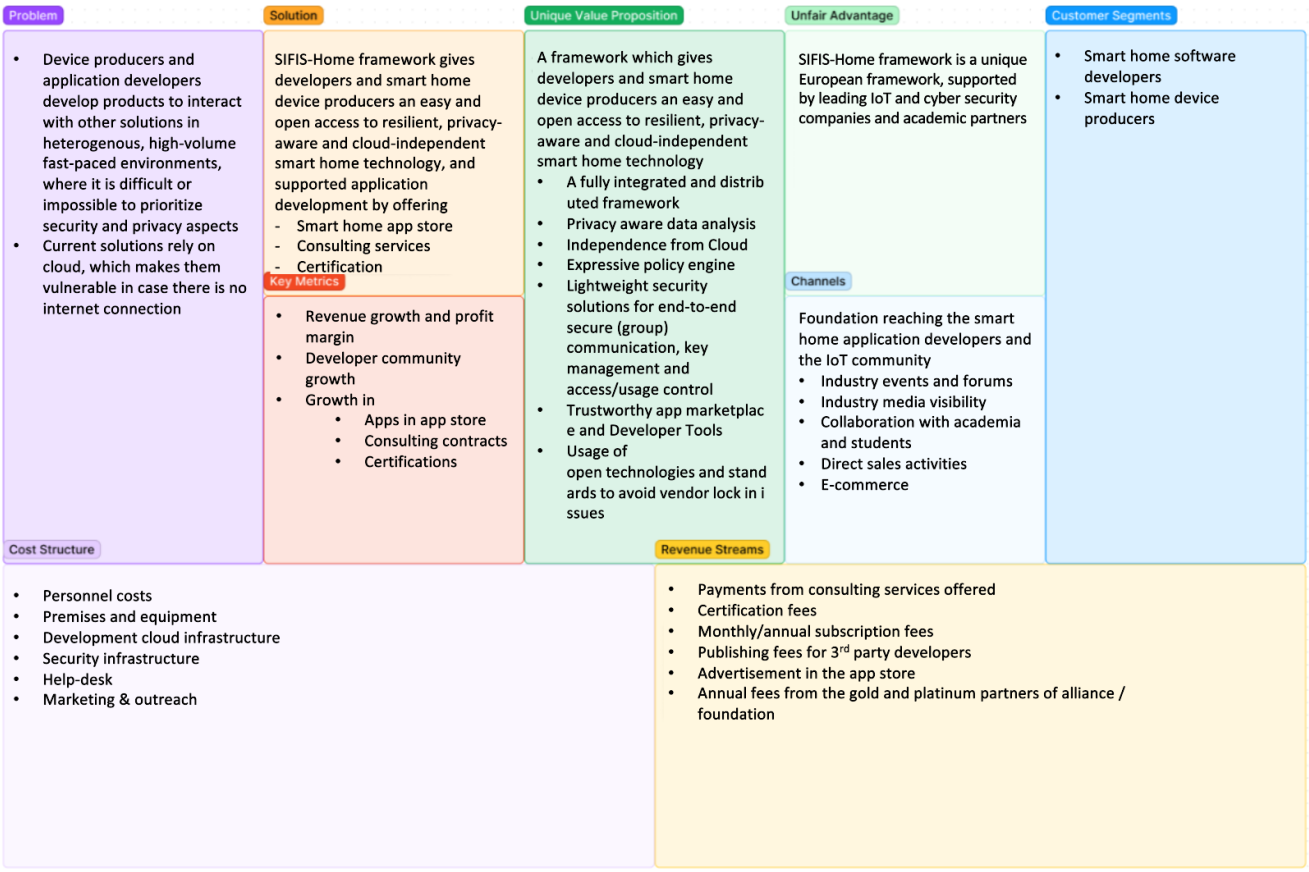


*Figure 7: Lean canvas for the SIFIS-Home framework, "the App store"*

### *Problem*

Smart-home application developers and device producers operate in a challenging environment, as discussed in Section 3.2. That is, the market is growing and offering great opportunities (see Section 2) but is also filled with heterogenous solutions. Developers and device producers develop products and services for an environment that is rapidly changing and where new and obsolete features and functionalities co-exist. Prioritizing the security and privacy aspects is difficult. In addition, current solutions rely on cloud, which makes them vulnerable in case a working Internet connection is needed to reach the service in smart home systems.

Consumers, i.e., the end users of the products and services developed by application developers and device producers, must choose between enjoying the functionalities of an interconnected smart home system (while potentially endangering their security, privacy and safety), and instead not being smart

home users altogether.

***Customer segments***

Customers for this business model are smart-home software developers and device producers, whose customers value their security and privacy. The targeted smart-home software developers and device producers have identified the problem discussed above and see market opportunities in addressing the problem (for more details, see the analysis of the market potential in Section 2.2 and the business scenarios and opportunities in Section 3.2).

Part of the marketing and communication efforts of this business model are bringing forth the current issues concerning security, privacy and safety of smart homes, and how the results of the SIFIS-Home project can be used to solve these issues. This strategy aims at increasing demand for secure and privacy-aware smart home solutions by increasing awareness among smart-home software developers, device producers and their end customers.

***Unique value proposition***

The SIFIS-Home framework gives developers and smart home device producers an easy and open access to resilient, privacy-aware and cloud-independent smart home technology, including

- A fully integrated and distributed framework
- Privacy aware data analysis
- Independence from Cloud
- Expressive policy engine
- Lightweight security solutions for end-to-end secure (group) communication, key management and access/usage control
- Trustworthy app marketplace and Developer Tools
- Usage of open technologies and standards to avoid vendor lock in issues

See Section 3.1, p. 24-25, for a detailed analysis of these value propositions.

***Solution***

The SIFIS-Home framework gives smart-home software developers and device producers an easy and open access to resilient, privacy-aware and cloud-independent smart home technology, and supported application development by offering 1) a smart home app store, 2) consulting services and 3) certification.

**Smart home app store.** The “Play Store” for smart homes allows third-party developers to develop applications and store them on the platform. For a developer developing IoT applications, the SIFIS-Home solution offers ways of controlling what the application is going to do, improving the privacy and security aspects of the application, and allows developers to more easily focus on the implementation of functionalities.

**Consulting services.** Smart home software developers and device producers are supported by offering them consulting services. These consulting services address, for instance, the issues related to knowledge, time, and commitment required to fully utilize open-source software.

**Certification.** Certification addresses the need to prove the trustworthiness of the solutions. SIFIS-Home certified products and services are guaranteed to be resilient, secure and privacy-aware.

This solution is provided by a partner or a set of partners of the alliance with a suitable customer interface and capabilities.

***Channels***

The alliance, introduced in Section 5.2, offers a channel for reaching the smart home application developers, device producers and the IoT community. The marketing and sales efforts can be supported by:

- Industry events and forums
- Industry media visibility
- Collaboration with academia and students
- Direct sales activities

The main sales channel for this business model is e-commerce.

***Revenue streams***

This business model offers customers complementary services creating several revenue streams:

- Consulting services provide opportunities to reach a revenue stream of 100 KER for each employee.
- Certification fees can be, depending on the selected model, as high as 5-15k for each B2B customer.
- Monthly/annual subscription fees can be between 5-20 EUR to the end users (as a comparison, Nabu Casa charges 6,50 USD monthly) and significantly higher for B2B customers.
- One-time publishing fees of 20-50 EUR for third-party developers, depending on the volume.
- Annual fees from the gold and platinum partners of alliance 2000 EUR and 10000 EUR, respectively

Furthermore, additional revenue can be generated through advertisement in the app store, which is a volume-dependent business model. If the app store is successful and the volume of end users increases considerably, this may be worth an annual revenue of millions of euros.

As the business grows, subscription-based fees enable exponential revenue growth potential, since every new installation provides new opportunities. For instance, Nabu Casa had an annual revenue of $4 million in 2021. If the business is shared between many companies and the estimated total revenue in the Smart Home market is +$100bn, then SIFIS-Home could take a $100M share within 5 years from now by providing an EU-based secure open-source ecosystem.

***Cost structure***

The main costs of the business model are the following.

- Personnel costs: on average, personnel costs are 50-80 kEUR per person yearly, depending on the country of operation and the required expertise level.
- Premises and equipment: approximately 10% of the personnel cost.
- Development cloud infrastructure: this cost depends on the volumes and the selected operator. Cloud server costs start from 50 kEUR per month.
- Helpdesk: One helpdesk employee is needed for every 1000 customers, and the cost per person is approximately 50 kEUR yearly.
- Marketing & outreach: the marketing budget is between 5-25% of the company's revenue targets. The final marketing budget depends on the company size and growth targets.

***Key metrics***

The performance of the business is measured by several key metrics, including

- Revenue growth and profit margin
- Developer community growth
- Growth in
    - Apps in app store
    - Consulting contracts
    - Certifications

***Unfair advantage***

The SIFIS-Home project and the planned follow-up project comprising several SIFIS-Home partners give this business model an unfair advantage, because they enable the SIFIS-Home framework to become a unique European framework, supported by leading IoT and cyber security companies and academic partners.

# 6 Partners' Exploitation Plans and Activities

Consistent with the objective 7 of the SIFIS-Home project, this section outlines the defined exploitation plans from the project partners on their individual intended usage of the project results, in order to reach a larger set of users and improve know-how, business and revenue.

**Consiglio Nazionale delle Ricerche (CNR)**

The topics addressed in SIFIS-Home are key topics for the Trust, Security and Privacy research unit of CNR. Being the most relevant Italian public research institution, CNR aims at exploiting SIFIS-Home to increase the interest of research and industry community in the research topics of distributed cybersecurity and trust, privacy preserving data analysis and fault tolerant architectures. In the first year of SIFIS-Home, CNR has learned about the challenges of converting existing real life centralized IoT architectures into efficient distributed fault tolerant systems. These challenges have motivated novel research work and initiatives for technological transfer activities, which are considered by CNR an important exploitation result. Following the activities in SIFIS-Home, CNR has strengthened existing connections and acquired new ones, both inside and outside the consortium, especially by exploiting joint project initiatives that have happened in the last months.

CNR aims at exploiting 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.

The exploitation plan has been fully implemented by CNR. For what concerns the increase of interest for research and industry community, it has been achieved by participating and organizing a number of events addressing both scientific and industrial community, including seminars and news coverage. Moreover, CNR has participated in the activities toward the W3C community lead by LUM, and in IETF lead by RISE. Through these activities, CNR disseminated the advantages of distributed and resilient IoT architectures with respect to centralized ones and the importance of privacy preserving data analysis. Through the activities of the project, relevant research papers authored or co-authored by CNR have been published in top level journals and conferences.

On the topics of SIFIS-Home, CNR has finalized, in collaboration with POL, two national project proposals, which have been funded by the Italian Government. The accepted projects are part of the prestigious program PRIN (Progetti di Rilevante Interesse Nazionale), and they aim at exploiting and maturating core elements derived from the SIFIS-Home project, such as the evaluation of application-related risks and the Privacy Dashboard.

Concerning the exploitation of technical results, CNR founded a spin off company during the project activities, as devoted to commercializing a software framework inspired by the principles of the SIFIS-Home architecture.

**Ericsson AB (ERI)**

Ericsson is one of the leading providers of Information and Communication Technology (ICT) to service providers. Ericsson is participating in the SIFIS-Home Research and Innovation Action as a research organization with project participants from Ericsson Research, and the main contribution is in the network and system security research on secure, interoperable, and robust communication, and security lifecycle management. As part of the SIFIS-Home project, Ericsson and RISE are driving the research and standardization of lightweight security protocols and enablers that simplify interoperability and integration of security services in any IoT application. The results include novel, secure and privacy friendly IoT architectures enabling consistent trustworthy and accountable authentication, authorization and accounting services across all IoT devices/ecosystems with enhancement of Public Key Infrastructures (PKIs) aiming to support PKI services (e.g., registration, revocation) for IoT devices. Specific examples of security components include the lightweight authenticated key exchange protocol EDHOC and the constrained-environment friendly authorization framework ACE-OAuth.

The deployment of these results is expected to increase the trustworthiness of Smart Home deployments and, in turn, the proliferation of high availability ICT services in homes. Moreover, the standardization of this innovative technology offers large scale exploitation of interoperable solutions beyond individual company products or presentations at industrial events. By targeting the core Internet and the high-security profile standards defining organization IETF, the impact of a new standard has a high potential to be deployed by technology companies world-wide and by other SDOs, like 3GPP, OMA SpecWorks, ETSI, GlobalPlatform, etc.

An indication of the exploitation achievement resulting from this work is the willingness of different industrial and academic stakeholders to invest time and resources into this development. A measure of success of exploitation is how convincing the results of this project are as perceived by other stakeholders, including project partners, other industrial partners, and subsequently, customers.

Ericsson intends to exploit project results in collaboration with industry partners, through proof-of-concepts and by raising industry awareness. For Ericsson, like other IoT service providers, device manufacturers, etc., the benefits of scale are important, and the use of common standardized technologies is a pre-requisite. During the execution of the SIFIS-Home project, Ericsson divested its IoT Accelerator business (Q1 2023) and is now working in this area through partnerships. One example of a company that has adopted an important security component developed within the SIFIS-Home project is given in [1]. This technology is exploited in their Centrios branded smart locks [2]. Other technologies standardized through the project and examples of partners adopting these technologies are presented in [3].

[1] ASSA ABLOY presentation of EDHOC at the LAKE working group, IETF 113, March 21, 2022 starts at 33:30 in https://www.youtube.com/watch?v=9cZ2oJ4KDxQ

[2] https://www.centrios.com/

[3] ACE-OAuth: A new standard for lightweight authorization and access control – Ericsson blog, https://www.ericsson.com/en/blog/2023/7/ace-oauth-standard-for-lightweight-authorization

**F-Secure Oyj (FSEC)**

F-Secure exploits the project results, and particularly SIFIS-Home AUD, within its connected home security offering, 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 its 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 will improve IoT security and privacy of the large customer base globally.

The organic new router deployments described in Section 2 are one channel that F-Secure is planning to exploit in order to bring Connected Home Security into the market. Communications Service Providers (CSP) almost without exception include the residential broadband router as part of their broadband service and F-Secure is partnering with the CSPs for delivering cyber security for Smart Homes globally.

Furthermore, F-Secure explores possibilities of exploiting new smart domains such as smart vehicles or connected cars, smart ships, smart cities, as part of another EU Horizon 2020 research project, *InSecTT*[13]. Connected cars can be thought of as mobile extensions of the connected home where end-user devices, such as mobile phones of the family members and guests may interact with the car's entertainment and other systems. F-Secure currently deploys Connected Home Security technology in consumer residential Internet gateways. These devices include Wi-Fi routers delivered as part of the broadband services by ISPs and telecommunication operators. Similarly, the Internet gateways found in vehicles could be equipped with IoT security technology. Discussions within *InSecTT* partners have taken place and we plan to further explore opportunities for expansion. The vehicle internal IoT system, not directly exposed to the users or passengers, has much more well-defined communication patterns with the outside world than the system exposed to the users. Therefore, the Manufacturer Usage Description (MUD) standard defined by the IETF is well suited for detection of potentially malicious anomalies in communications.

In addition, F-Secure has participated in industry and partner events to showcase the results of the project and collect feedback from potential customers. These events include Broadband Forum events, F-Secure's annual partner event SPECIES, International Cybersecurity Forum and Prpl Foundation events.

**Intel Deutschland GmbH (INT)**

[13] For further information, please visit: https://www.insectt.eu/domains/automotive/.

INT has a strong focus on innovation capabilities related to AI / Machine Learning (ML) and IoT topics, especially in the Industrial IoT and Smart cities paradigms. In addition to supporting open-source contributions, INT plans to improve components used in the project in order to achieve the best possible performance and richness of the feature set. Outcomes and feedback of the project will be taken into account in order to improve the quality of each particular component, so that such back-to-product contributions will have a wider and longer by time impact through the industry, our partners and developers. Marketing and additional contribution channels will be used to support and promote the project across different aspects, industry events and communities.
The broad coverage of several standards will allow Intel to push SIFIS-Home technologies and innovation to not yet touched standard bodies, e.g., 3GPP or ETSI, which are planning to extend the range of their work towards smart and secure cities activities.
Needed HW and SW stack recommendations will be proposed and shared, as focused on the needs of the project and to fulfil rich features set and needed level of functionality.

**Intelligentsia Consultants Sarl (IC)**

IC is specialized in managing R&D and innovation projects. The company expected that the successful support for the SIFIS-Home project would stimulate further project management assignments. Indeed, this has been the case, IC went on to be requested to write an EIC pathfinder open proposal, which was selected for funding and the company will assist with the administrative management and dissemination activities. At the end of the SIFIS-Home project, IC was also assisting CNR with the preparation of several Horizon Europe proposals with a focus on collaborative and trustworthy frameworks for reliable maritime cyber risk management.

**Luminem SRLs (LUM)**

LUM is a small Italian SME. It focuses on system development and safer implementation of open-source 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 means to enforce the best software engineering practices.

The company joined the W3C and is contributing to the WoT specification effort with its brand new Rust implementation of the WoT standards.

The company plans to offer consulting services for companies that want to offer connected versions of their line of products, both to train their teams and to offer solutions based on the **wot-rust** platform.

**Domo**

DOMO is the main author of the SIFIS-Home DHT and of the WoT compliant firmware for the IoT

devices used in the project pilot. DOMO released both components as open-source software and will support implementors willing to use them in their projects.

**Riots Global Oy (RIO)**

Riots is a Finnish SME IoT company that manufactures various products and SaaS service used in smart buildings. 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. We see IoT security as a crucial topic in smart homes and other similar infrastructures in the near future. Our interest is in developing and offering functioning, secure, and reliable IoT solutions for wide commercial use. Riots is especially interested in the concept and implementation of privacy in smart buildings – a wide concept with a vast number of smaller components and several levels of users. One of our main focus points is the challenge of ensuring the secure and correct distribution of rights to access different sets of the collected data, and of ensuring the integrity of the network as a whole against malicious actions. In addition, in order to strengthen our own product security, Riots wants to be involved in creating best practices and quality standards when it comes to IoT security.

Possible implementations of the SIFIS-Home project regarding Riots' expertise and focus on the project could include the following products, which could fit in the growing market of home and building automation:

- Real-time Traffic Analyzation Service
    - SaaS solution for businesses
    - Analyze data in real-time for malfunctions and anomalies
    - Provide solutions based on the results of the analysis
    - Increase network and user security preventing data leaks and software attacks
- Smart Thermostat and HVAC Control
    - Detect whether user is at home or not and adjust conditions based on that knowledge
    - Learn from user behavior to adjust indoor conditions proactively

**Sensative AB (SEN)**

Results from the SIFIS Home project are a vital part of the Sensative Yggio strategy, are continuously getting commercially exploited, and are already available in the public commercial Yggio servers at https://beta.yggio.net, https://yggio3-beta.sensative.net as well as at the production level server https://public.yggio.net , as well as in several customer private Yggio installations.

The results include both: i) the heart of Sensative Yggio, which is the FIWARE compliant open-source

RATATOSK publish / subscribe Context Broker that is being enhanced as part the project and that will manage information about the status and meta data of devices connected to the SIFIS-Home system ; and ii) configuration-related data needed to maintain the integrity of the system. An additional result is the new mobile-phone-adapted UX of Yggio, including the Device Manager, the Market Place, and the upcoming alarm/log functionality, as driven by the UI design developed in SIFIS-Home.

To summarize, except for our primary exploitations plans to extend Yggio with the SIFIS-Home UX technologies (Devices, Dashboard, Market Place, Alarm/Log) and anomaly detection capabilities, we also see the following future opportunities depending on commercial market interests:

- Extend Yggio with WebOfThings support
- Extend Yggio with CoAP + Group OSCORE support
- Extend Yggio with DHT support
- Extend Yggio with analytics for intrusion detection

SENS plans to actively promote all the results of the project to our customers, partners and ecosystem of service providers including in the FIWARE OiL iHub. This will be done both in specific meetings with partners and customers as well as in more general types of events for multiple partners, customers or open events. SEN has municipalities, utility companies, real estate companies and home builders as customers, and 15-20 service provider partners in domains such as smart home, smart building, waste management, smart agriculture, sustainability reporting and smart shipping.

**RISE Research Institutes of Sweden (RISE)**

RISE is a research institute and, as an outcome of Research & Development (R&D) activities, it produces know-how, publications, specifications and software components as project results.

Exploitable results include: preventive and reactive cybersecurity lightweight solutions; related proof-of-concept SW implementations also used to yield preliminary assessments; their transfer to project demonstrators/pilots; as well as standard proposals submitted and considered within the international open standardization body Internet Engineering Task Force (IETF).

Specific solutions and outcomes from RISE focus on lightweight security protocols and methods for secure end-to-end (group) communication, management of cryptographic keying material and fine-grained enforcement of access control policies. These are documented in the project Deliverables D3.3 "Final report on Network and System Security Solutions", D7.4 "Final Dissemination Report" and D7.5 "Final Standardization Report".

RISE will exploit the project results according to a research exploitation model. This includes especially the following exploitation actions, which are expected to be carried out also beyond the end of the SIFIS-Home project.

- Dissemination of research and development results through academic publications. This will target high-quality international journals, conferences and workshops, as well as tutorials and seminars.

- Contribution to open standardization activities, with particular reference to the international body Internet Engineering Task Force (IETF), and especially to its Security- and IoT-related Working Groups, such as ACE, CoRE, LAKE and SCHC.
  These activities and their outcomes are in turn expected to indirectly contribute towards other international standardization bodies - such as Open Mobile Alliance (OMA) and 3GPP - that rely on IETF standards as building blocks to develop their specifications. This will create opportunities for interactions and collaborations with these organizations, in order to facilitate the use, profiling and adaptation of considered IETF standards.
  Furthermore, in the spirit of open standardization, the availability of such standard cybersecurity solutions will greatly facilitate the building of a cohesive ecosystem of different vendors, by ensuring interoperability of their different products and avoiding a lock-in effect.

- Integration of software components into official open-source software libraries as well as into further related R&D activities.
  It is especially planned to target the integration of the RISE open-source implementations of the Group OSCORE and EDHOC security protocols into the open-source library Californium from the Eclipse Foundation, which already provides the CoAP protocol and the OSCORE security protocol. See https://github.com/eclipse/californium
  It is also expected that, building on such implementations, further related security solutions can also be implemented, which in turn would open for their potential integration in larger software libraries, such as Californium.
  The availability of such open-source implementations for open standard security protocols is expected to further accelerate the building of a cohesive ecosystem of different vendors mentioned at the previous point, as well as to enable and facilitate related R&D activities building on those.

- Establishment of new and reinforcement of current collaborations for joint research and dissemination activities. This will strive to target both Swedish and international partners, from both the industry sector and the academia.

- Enhancement of competence and expertise in cyber security, with particular reference to the IoT and smart environment application/network domains.

- Participation in future Research and Innovation projects as well as Innovation projects, whose topics and activities comprise IT-security. This will strive to target the participation to both Swedish and European projects as a core partner, and to leverage the experience and outcomes from the SIFIS-Home project as assets to further build on.

In addition to RISE itself, the results from the exploitation actions mentioned above are intended to benefit and target especially two customer segments, namely the "IoT industry" and the "Research community".

As to the "IoT industry", results from RISE will benefit the overall offer of IoT services and products, by fostering the availability of high-quality security solutions, open standards and early open-source implementations, leveraging the support and efforts of open collaborative communities. As mentioned above, this will ultimately contribute to building a cohesive ecosystem of vendors within the IoT application domain, thus speeding up and greasing the commercialization of secure IoT-based applications.

As to the "Research community", results from RISE will benefit the overall availability of findings and results on cybersecurity topics, especially with respect to lightweight security protocols and methods for the IoT. To this end, practical means include accessible related works and documentation (e.g., academic publications and technical specifications/reports), as well as of open standards and software implementations. This will yield a more vivid and productive research community, which will thus enjoy higher chances to progress the state of the art in the field in a more effective way.

**Centria University of Applied Sciences (CEN)**

Centria University of Applied Sciences is located in three different campus areas in Ostrobothnia, Finland, which ensures a wide operational environment with plenty of partners and local businesses. Centria's Research and Development has expertise in the fields of wireless networks and systems, positioning, cybersecurity and embedded systems. Centria possesses a strong know-how in working with industrial Internet and intelligent traffic applications, as well as mobile networks – especially in testing mobile networks. Centria has been running around 100 Research & Development projects each year, and has a strong expertise in local, national and international funding sources. Centria is widely involved in both national and international projects. Centria provides expertise in data security management to SMEs.

Centria University of Applied Sciences uses the results of SIFIS-Home for courses in computing sciences as well as for IoT-related topics. Currently there are two courses running in the academic year 2022-2023 that utilize the knowledge gained from the SIFIS-Home project, with 61 students enrolled on them. In addition to domestic and international students, Centria also educates and organizes training courses for businesses, unemployed individuals and those who are already employed but intend to enhance their skillsets. In the academic year 2022-2023, Centria has organized instances of continuing professional development training in cyber security. Further sessions of continuing professional development are planned and scheduled for the upcoming semesters. As the target group of Centria's various educational opportunities is wide and most are offered also with the possibility of remote participation, the knowledge gained in the SIFIS-Home project has a great potential to reach businesses and people working in many different industries.

Centria has contributed to SIFIS-Home by producing academic journals and conference papers, particularly in the important research field of anomaly detection in network traffic. These contributions will lead to a better understanding of cyber risks and cyber risk prevention in IoT environments, as well as higher security of smart home systems. In addition to academic publications, Centria has had an active role in publishing articles in newspapers, magazines and online platforms in English, Finnish and Swedish to educate businesses, academics and individuals in cybersecurity issues and creating a better understanding of the importance of security solutions also outside of technology oriented research community (e.g., end users, consumers, new businesses, SME's from all industries, teachers and other faculty members within Centria and partner organizations).

Using the project results, Centria will arrange workshops for selected SME's and micro size entrepreneurs to spread knowledge about the project results to the Centria´s operational area. During 2022-2023, the SIFIS-Home project has been presented in a number of different events: at Centria DropIn, an open day event for students and local companies, were Centria´s cyber security experts raised the importance of cyber security in smart homes; at a hybrid event SecTalk, where reearch in SIFIS-Home was presented to local SME´s and students; at the Valentine´s Day networking event together with local companies, where Centria contributed to cyber security discussions. Centria also visited the regional Energy Festival. The webinar organized by SIFIS-Home "Increasing Cybersecurity and Empowerment in the Digital Environment in Europe" provided evidence of European cooperation in cybersecurity. Future events are planned in order to raise and spread the understanding of IoT and smart home cybersecurity issues to the businesses located in Centria's geographically wide operational area.

The exploitation actions of Centria are intended to benefit the operational area of Centria University of Applied Sciences. This includes all the stakeholders of the three regions where Centria has an active presence. The project actions are focused on research activities, but an additional goal is also that the knowledge gained within the SIFIS-Home project reaches local companies, students and possible other groups that benefit from better understanding of cybersecurity issues in IoT and smart home environments. The project results will also be used in preparatory work for upcoming projects, where state-of-the-art knowledge is needed.

**Politecnico di Torino (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. The 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.

In particular, POL holds 5 courses related to the topic of IoT, 2 at BSc level, 2 at MSc level and 1 at PhD level for a total of approximately 420 students.

In the context of these courses, seminars are planned for the A.Y. 2022/2023 on the following topics:

- WebOfThings
- Code quality for IoT software
- Privacy in the Smart Home

POL aims to exploit the SIFIS-Home project results with a research model, which includes disseminating the research results through academic publications, contributing to open-source projects (e.g., rust-code-analysis maintained by Mozilla) and collaborating in dissemination activities with national and international partners from academia and the industry.

In parallel, POL plans to exploit technological results through possible spin-off activities.

# 6 Conclusion

The SIFIS-Home project and its results have significant implications for business opportunities in the areas of Smart Home security and IoT security, with a high European and international market demand, as both the IoT paradigm becomes more widespread, and the importance of properly addressing cybersecurity and privacy continues increasing.

In particular, as IoT technology and various Smart Home systems are becoming more commonly adopted, the attack surface against those increases and creates new risks. This is an issue which customers and manufacturers might not adequately understand and be able to tackle, and therefore there is a need for the SIFIS-Home solution and its components. The efforts detailed in the Deliverable D7.4. *Final Dissemination Report* are in strong connection to the activities described in this report in addressing the challenges above by raising awareness and increasing trust towards secure smart home and IoT systems via various dissemination and communication activities. In addition to increasing trust among the users of smart home systems, the trend also emphasizes the need for standardized protocols that are highlighted in this report. Detailed activities of SIFIS-Home partners regarding standardization are provided in the Deliverable D7.5 *Final Standardization Report*.

This document has summarized the business and exploitation plans and strategies to utilize the results of the SIFIS-Home project after the project completion by analyzing related business scenarios and opportunities. It describes the considered exploitation strategy, the analysis of the smart home market, the developed business scenarios and models, the identified KERs, the analysis of the exploitation potential of the project results, as well as the planned specific business and exploitation of the main project results (especially the SIFIS-Home framework) and partner specific exploitation activities and plans.

# 7 Annex A: Glossary

| Acronym | Definition |
|---|---|
| ACE | Authentication and Authorization for Constrained Environments |
| AI | Artificial Intelligence |
| AIxIA | Italian Association for Artificial Intelligence |
| AUD | Aggregated Usage Description |
| BMC | Business Model Canvas |
| CSP | Communications Service Providers |
| CoRE | Constrained RESTful Environments |
| DDoS | Distributed Denial of Service |
| DHT | Distributed Hash Table |
| GMQ | Gartner Magic Quadrant |
| IA | Innovation Action |
| IETF | Internet Engineering Task Force |
| IoT | Internet of Things |
| KER | Key Exploitable Result |
| LAKE | Lightweight Authenticated Key Exchange |
| MUD | Manufacturer Usage Description |
| NSSD | Not So Smart Devices |
| OS | Operating System |
| IP | Intellectual Property |
| IPR | Intellectual Property Rights |
| RIA | Research and Innovation Action |
| SCHC | Static Context Header Compression |
| SHFQ | Smart-Home Framework Quadrant |
| SIFIS-Home | Secure Interoperable Full-Stack Internet of Things for Smart Home |
| SME | Small and Medium Sized Enterprise |
| SPOF | Single Point of Failure |
| WOT | Web of Things |
| WG | Working Group |
| WP | Work Package |

## References


ABB-free@home (2022). Website. https://new.abb.com/low-voltage/products/building-automation/product-range/abb-freeathome/system/features

Amazon Alexa (2022). Website. https://www.amazon.com/alexa-smart-home/b?ie=UTF8&node=21442899011

Clauser, G (2019). *Amazon's Alexa Never Stops Listening to You. Should You Worry?* The New York Times. https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/

European Research Executive Agency (2023). Website. https://rea.ec.europa.eu/horizon-europe-how-apply_en#types-of-projects

Fagan, M., Megas, K. N., Scarfone, K. & Smith, M. (2020) *Foundational Cybersecurity Activities for IoT Device Manufacturers.* National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8259

Fortune Business Insights (2022). *Smart Home Market Size, Share & COVID-19 Impact Analysis, By Product (Home Monitoring/Security, Smart Lightning, Entertainment, Smart Appliances and Others) and Regional Forecast, 2021-2028.* Market research report, report ID: FBI101900, 120, 2/2022. Read more at: https://www.fortunebusinessinsights.com/industry-reports/smart-home-market-101900

Frost & Sullivan (2021). *Market Opportunities for Cybersecurity*. Executive report, prepared for Business Finland. November 2021.

Google Home (2022). Website. https://home.google.com/welcome/

Grand View Research (2022). *Smart Home Market Size, Share & Trends Analysis Report By Application* (Security & Surveillance, Lighting, Entertainment, Energy Management, HVAC, Smart Kitchen, Home Fitness & Wellness), By Region And Segment Forecasts, 2022-2030. Smart Home Market Share & Size Analysis Report, 2022 - 2030 (grandviewresearch.com)

Hyppönen, Mikko (2021). *Internet*. Helsinki: WSOY, ISBN 978-951-0-46441-0.

Maloney, M., Reilly, E., Siegel, M., & Falco, G. (2019). *Cyber physical iot device management using a lightweight agent*. In 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1009-1014). IEEE.

Osterwalder, Alexander; Pigneur, Yves; Clark, Tim (2010). Business Model Generation: A Handbook For Visionaries, Game Changers, and Challengers. Strategyzer series. Hoboken, NJ: John Wiley &

Sons. ISBN 9780470876411. OCLC 648031756. With contributions from 470 practitioners from 45 countries.

Partha, P. R. (2016). *A survey of iot cloud platforms*. Future Computing and Informatics Journal, 1(1-2):35– 46, 2016.

Statista (2021). Digital Markets, Smart Home, Worldwide. Smart Home - Worldwide | Statista Market Forecast

World Bank (2021). Fixed broadband subscriptions International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database
https://data.worldbank.org/indicator/IT.NET.BBND