D7.3

Preliminary 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: 31/03/2022
Actual submission date: 31/03/2022

22/2/2022
Version 1.8

Responsible partner: FSC
Editor: Tuuli Lindroos
E-mail address: tuuli.lindroos@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: Tuuli Lindroos (FSEC), Marco Tiloca (RISE), Göran Selander (ERI), Laura Palovuori (CEN), Luca Barbato (LUM), Håkan Lundström (SEN), Samuli Stenudd (RIO)

Approved by: Elina Hirvonen (CEN), Göran Selander (ERI)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	6/10/2021	Initial ToC	FSC	All
0.2	13/11/2021	Content from RISE	RISE	All
0.3	29/11/2021	Content from FSEC	FSC	All
0.4	30/11/2021	Content from ERI	ERI	All
0.5	8/12/2021	Content from CEN	CEN	All
0.6	9/12/2021	Content updated 1.2. Methodology	CEN	All
0.7	17/12/2021	Contribution to 3. Business Scenarios	LUM	All
0.8	17/12/2021	Contribution to 3. Business Scenarios	ERI	All
0.9	20/12/2021	Contribution to 4 Exploitation and activities	SEN	All
1.0	20/12/2021	Contribution to 3. Business Scenarios	RIO	All
1.1	20/12/2021	Contribution to 3. Business Scenarios	FSC	All
1.2	19/1/2022	Content from CNR	CNR	All
1.3	19/1/2022	Content from INT	INT	All
1.4	20/1/2022	Content from POL	POL	All
1.5	21/1/2022	Content from RIO	RIO	All
1.6	18/2/2022	Review comments from CEN	CEN	All
1.7	21/2/2022	Review comments from ERI	ERI	All
1.8	22/2/2022	Processed review comments	FSC	All

Executive Summary

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 security, 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 and trust of smart home systems and end users.

This deliverable provides the *Preliminary Business and Exploitation Plan* with a focus on paving the way to sustainable exploitation after the project completion. Furthermore, this deliverable provides the exploitation strategy including exploitation objectives and methodology, market analysis including the market potential, trends and players, potential business scenarios and individual partners' exploitation plans and activities. The exploitation strategy aims at producing a Quantified Business Plan that ensures the solutions developed in the project remain viable and sustainable after the project has run its course.

Consistent with the objective 7 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 privacy-aware Smart Home applications. This will be achieved by exploiting the influence on the internal, European and international markets of the industrial partners in the consortium, which includes main players in the IT and IoT security market.

The exploitation strategy described in this document is structured to provide, based on the mission statement of the SIFIS-Home, the outlook to the exploitation objectives describing the main goals of exploitation in SIFIS-Home and the main methodology outlining different ways of reaching the exploitation objectives. The exploitation strategy provides the basis for implementing and replicating the new solutions and technologies in a broader context.

Table of contents

1 Exploitation objectives and methodology

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 management of security and safety in Smart Home system. SIFIS-Home provides both: development APIs compatible with a major commercial IoT architecture for development of certifiable, secure and privacy-aware applications; and 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 trust, acceptance, and building confidence in the fact that home automation solutions are truly secure and safe to use in terms of data security and integrity. As an underlying note, the SIFIS-Home project is a Research and Innovation Action (RIA) project, a corresponding business and exploitation plan will be provided considering the specific characteristics of such project type.

1.1. Objectives

This section explains the objectives of the exploitation in SIFIS-Home, in other words the main goals and targets of the exploitation activities.

The objectives of exploitation in SIFIS-Home can be described as the following:

- Monetizing the project solutions and maximizing the benefit from the project solutions financially
- Exploring future needs of the potential customers for further development of secure IoT through the project solutions
- Improving the research know-how and the state of the art
- Create general guidelines and framework to guide the overall development of secure IoT

Ensuring the replication of project results in various domains as listed in the examples above aim to maximize exploitation. The following section explains the different ways of reaching these objectives.

1.2. Methodology

This section provides the methodology of exploitation, by explaining different ways and practices of reaching the exploitation objectives presented above. The methodology describes the exploitation possibilities in a Research and Innovation Action (RIA) -project, which characterizes the distinct exploitation activities in SIFIS-Home.

Different options of exploiting the project solutions in SIFIS-Home can be for example the following:

- Usage of the developed technology and solutions in existing product offering
- Inclusion of technology developed in the project in relevant standards
- Receive direct feedback from potential customers of the real-life demonstrations produced in the project
- Usage of the project solutions know-how in research and teaching
- A follow-up Innovation Action (IA) project with higher technical readiness level and industry driven focus

Each option of exploiting the project solutions is described in more detail below.

Usage of the developed technology and solutions in existing product offering

The first option is exploitation and utilization of the technology developed in the project in the existing products (especially targeted for industrial partners) to further improve and develop the product and service offering. More detailed exploitation plans by each partner are described in the section 4.

Inclusion of technology developed in the project in relevant standards

As a far-reaching exploitation result, technology solutions developed in the project are being included in generic lightweight security standards suitable for all kinds of 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. As a standard in a recognized international SDO there is a high exploitation potential for industry and society. By also contributing to and encouraging the development of open-source implementations of these standards the threshold for deployment is significantly reduced.

Receive direct feedback from potential customers of the real-life demonstrations produced in the project

One form of exploitation from the technical and real-life demonstrations produced in the project is

the feedback received from potential future customers. These real-life demonstrations offer a valuable opportunity for the launching customers to build and learn from. This is done mostly through industry partners by utilizing the existing customer connections and attending various events during and after the project with potential future customers benefitting from the technology developed in the SIFIS-Home. Various events utilized here can include workshops, conferences, and other occasions where the partners are able to present the technical demos to the potential future customers and receive feedback of these demos. This method of exploiting the project results paves the way to the future exploitation by providing valuable insight based on the customers initial reactions and future needs on the field of IoT security.

Usage of the project solutions know-how in research and teaching

The project results will be exploited and used for research and development purposes as well as for teaching. In teaching the project results will be used for planning the content of courses and the results will be integrated into the courses and curriculums of the university. Smart home is also an interesting topic for thesis work as well as for journal papers, where the results can be utilized as well.

A follow-up Innovation Action (IA) project with higher technical readiness level and industry driven focus

As a last exploitation method, a follow-up Innovation Action (IA) project with higher technical readiness level and industry focus could be provided to increase the technical readiness level of the project solutions developed in the SIFIS-Home project for more effective and broader commercial exploitation purposes.

The guiding principles for exploitation are as follows:

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

Research Institutes intend to, in addition to publication activities and the reuse of results, transfer acquired technologies to third-party companies as a way of improving their level of competitiveness.

Industrial Partners intend to exploit the results of the project by introducing new policies, products, solutions and/or by integrating the newly developed technologies in their existing policies, products and/or solutions.

Detailed exploitation plans by each partner are presented in the section 4 of this document.

2 Market Analysis

This section describes the market analysis of the SIFIS-Home project results for exploitation and business plan, consisting of the analysis of market trends, players and market potential in different market levels. The section is divided into two subsections, first describing future market trends and players and second forecasting the market potential based on the analysis.

2.1. Market trends and players

The following section reflecting the market analysis context relies mostly on the recent publication[1] by the Chief Research Officer of F-Secure, Mikko Hyppönen. As F-Secure acts as the WP7 leader and D7.3 editor, this section mainly builds upon the expertise provided the experts in F-Secure and the insights provided by CRO Hyppönen reflect, to a large extent, the views of F-Secure. His long career in F-Secure together with key professionals and technology developed within the organization provides credible background and insights to the development and future trends of the IoT security.

In order to analyze the market potential, future trends and key players in IoT security, the existing trends and development of the digitalization and internet need to be reflected. 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, 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 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 trillion network connected devices, vastly expanding the attack 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), also referred as Not So Smart Devices (NSSM) in WP1 deliverable D1.1, meaning all possible devices that use electricity will be 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 transforming any device to the internet will be low enough to make the transformation cost-efficient. (Hyppönen 2021, 156.)

Resisting the IoT-revolution will be difficult or even impossible: it can be assumed that in the future

[1] Hyppönen, Mikko (2021). *Internet*. Helsinki: WSOY, ISBN 978-951-0-46441-0. Published on the 5th of October 2021.

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 through the internet by means we can directly control (e.g. Wi-Fi-network) but also most likely accessed through 5G or 6G connections. Therefore, the primary responsibility of securing the devices will be left for the manufacturers producing the devices. In other words, the manufactures of IoT devices, which in the future mean 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, the pricing of these more expensive secure smart devices becomes a challenge. (Hyppönen 2021, 157–160.) This trend also highlights the need for cyber security awareness raising and education.

In addition to the security threats associated with the proliferated vulnerability surface of increased number of smart devices[2] and compromise of not secured IoT devises[3], the loss of privacy becomes an 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 across various devices used by one user is combined, the 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 the 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 cyber security and privacy measures and processes for IoT platforms, environments and devices are not adopted.

2.2. Market potential

Based on this background described above, the market potential for secure IoT platforms is significant. According to a market analysis conducted already in 2016, there are nearly fifty different IoT platforms that at the time existed (Partha, 2016). The explosive growth of network connected devices and the fast development of IoT systems during recent years has only increased. However, the security considerations have not followed this development. IoT platforms face different concerns related to privacy and data transmitting, safety and security concerns which are amplified when IoT

[2] 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).

[3] For example, distributed denial of service (DDoS) attacks are increasingly plausible among not secured IoT devices in the face of evolving threats to compromise IoT devices and use them to harm device customers (Fagan, Megas, Scarfone & Smith 2020)

systems are built in smart homes, where they may cause physical damage and even threaten the privacy of individuals. Descriptive example of IoT security concern is their susceptibility to hostile takeover via botnet, which have proven to be effective (Maloney, Reilly, Siegel & Falco 2019). It can be deduced that without building trust in these devices through security considerations, the adoption of IoT devices can decelerate. Therefore, addressing the security-by-design approach from the beginning of manufacturing will have a high effect on the market potential of cyber secure smart home systems and smart devices. Manufactures will become the key players within this field.

Concerning the detailed market analysis and forecast of smart home security and solutions developed in the RIA SIFIS-Home project, the following analysis of fixed broadband connection households by F-Secure provides further insights. The number of households with a fixed broadband connection is estimated to reach over 1,2 billion in 2021 (World Bank 2021). By assuming a relatively conservative growth rate of approximately 4 % with a churn of 6 %, a minimum of 120 million 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 M figure. On top of the 1,2 billion households there is households with mobile broadband on 4G and growing 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[4]. Communications Service Providers (CSP) practically 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 the smart homes globally.

Based on the market analysis provided above, the following market levels are explored in order to guarantee the exploitation of the project results 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 academics, SMEs and industrial partners themselves present a significant market for the SIFIS-Home results to be deployed.

European market: In addition to the market provided by the end-user partners, the participating commercial and academic partners provide demo site workshops. 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) 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.

[4] For further details please see section 3.3. and section 4 describing F-Secure's exploitation plans.

3 Business Scenarios

This section describes the potential business scenarios related to the exploitation activities of the SIFIS-Home project explored after the first half of the project. The scenarios presented here are derived from the market analysis in section 2, considering the forecasts and analysis of the market potential, trends and players within the field of IoT security and Smart Home.

3.1. Interoperating security solutions

The technology landscape of the Internet of Things 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 either use products from one company, or an application framework from a specific platform provider. Also in that case, 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 if the various units support compatible protocols and formats. 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. This is of special relevance in terms of security: 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 to combined interoperability and trustworthiness is to specify a framework including security protocols that performs well independent of device capabilities. By enabling constrained devices to support a lightweight security framework which can be implemented during manufacture, there is less need for integration patching together existing security components built-in from manufacture with other security components common to the specific deployment. The latter has several disadvantages (potential mismatch between security components in device and deployment, additional sources for bugs, difficulty to reuse in other settings, less likelihood to scale, lower operating margins, etc.)

Ideally, such a security framework should be an international standard, widely available as open-source 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 standardization of generic lightweight security protocols
- Open-source software and interoperability testing with other implementations

- Tools, guidelines, and support for secure development and certification (see 3.2).

As a summary, one exploitation result of the project is to achieve better cost efficiency in protection of smart home deployments with the help of standardized security solutions using available code implemented during manufacture through best practices.

The exploitation achievement resulting from this work can be measured in terms of the willingness of different industry 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 others, including project partners and other industrial partners, and subsequently, customers.

3.2. Developer tools and certification

One of the key problems with the development of trustworthy IoT solution is that the developers might be aware of the best practices but for ready-to-market constraint voluntarily decide to give up on some of them to reduce their development-to-market cycles, 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 there are fewer reasons to not use them.

The key components 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 did not used to have 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 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.

3.3. Connected home security

Within the smart home security domain, the primary aim of the security framework is to provide security and protect the household residents. This connected home security business scenario is part of larger entity of 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 from 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 risk 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 household 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.

The 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[5] about consumers and their behaviors in the

[5] 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

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.

3.4. 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 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. They are expected to develop applications and services for 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 contain 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 an additional requirement on top of the more traditional ones including 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 involving MUD concept, an increased level of security can be provided by knowing the manufacturer intended behavior when monitoring and verifying actual observed behavior

---

results: https://www.f-secure.com/content/dam/f-secure/en/partners/operators/resources/operator-resources_CHS-infographic.pdf.

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 similar model used in broadband routers: defined mandatory and optional security requirements on routing devices[6]. 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[7] about consumers and their behaviors in the connected home area confirm the potential of the business scenario by describing consumer needs within the smart home area as follows:

- Consumers don't trust smart device manufacturers: 80% think manufacturers are not doing enough to ensure online security and privacy of smart home devices
- 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[8] confirming the analyzed business potential within the field and being an emergent area creating new market opportunities in the future.

[6] For further details, please see: BSI TR-03148:Secure Broadband Router (bund.de).
[7] 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.
[8] 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).

3.5. Smart home business acceleration services

The SIFIS-Home project focuses on creating Secure Interoperable Full-Stack Internet of Things for Smart Home. As result there is a substantial number of problems solved and implemented solutions in the Smart Home scene. All the public deliverables of the project will be open-source, meaning anyone can utilize the results. However, the result will be a huge piece of software and information that will require knowledge, time, and concentration 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 SIFIS-Home, containing the following:

- 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 SIFIS-Home architecture as a service so customers can focus on parts that are most useful for their business scenarios
- Various advertising scenarios that can be added to platform

4 Partners' exploitation plans and activities

Consistent with the objective 7 of the SIFIS-Home project, this section outlines the defined exploitation plans from project partners on their individual intended usage of project results 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 in 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 of the consortium, especially by exploiting joint project initiatives that 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.

Ericsson AB (ERI)

Ericsson is one of the leading providers of Information and Communication Technology (ICT) to service providers. As part of the SIFIS-Home project Ericsson is driving the research and standardization of lightweight security protocols and enablers that simplify interoperability and integration of security services. The deployment of these results is expected to increase the trustworthiness of Smart Home deployments and, in turn, the need for high availability ICT services in homes.

Ericsson also intends to exploit project results in collaboration with industry partners, through proof-of-concepts and by raising industry awareness. A candidate product for use of project results is the Ericsson IoT Accelerator platform for device and data management.

F-Secure Oyj (FSEC)

F-Secure intends to exploit the project results to its connected home security offering, in particular, the F-Secure Sense router SDK. The offering is provided to router makers and service providers to embed the SENSE router SDK into their own routers. FSEC is currently protecting tens of millions of

consumers through our 200+ service providers and telecom partners and the project results are exploited to the customer and partner bases. Therefore, integration of the project results to Sense router SDK will improve IoT security and privacy of the large customer base globally.

The organic new router deployments described in the section 2 are one channel that F-Secure is planning to exploit in getting Connected Home Security into the market. Communications Service Providers (CSP) practically 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 the Smart Homes globally.

Furthermore, F-Secure aims to explore 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*[9]. Connected cars can be thought as mobile extensions of the connected home where end-user devices, such as mobile phones of the family members and guest 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. Initial 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 communications 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 explores the possibility of collecting feedback from potential customers of the technical demonstrations developed in the project. Potential connected home security related events where F-Secure is planning to attend during years 2022-2023 where demonstrations could be showcased to potential customers to receive feedback for future needs and initial review of the technical end results of the SIFIS-Home project are currently assessed.

Intel Deutschland GmbH (INT)

INT has strong focus at innovation capabilities related to ML and IoT topics. Beside support of open-source contributions INT plans to improve components used in the project in order to achieve best possible performance and richness of the feature set. Outcomes and feedback of the project will be taken to improve quality of each particular component, so such back-to-product contributions will have wider and longer by time impact through the industry, our partners and developers. Marketing and additional contribution channels will be used to support and promote the project across different aspects, industry events and communities. Needed HW and SW stacks recommendations will be proposed and shared as focused on the needs of the project and to fulfil rich features set and needed

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

level of functionality.

Intelligentsia Consultants Sarl (IC)

IC are specialized in managing R&D and innovation projects. The company expects that successful support for the SIFIS-Home project will stimulate further project management assignments.

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 mean to enforce the best software engineering practices.

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 Webthings/WoT platform.

Mind SRL (MIND)

Mind Home is a multi-gateway solution to manage devices inside the smart home. Current state-of-the-art solutions have been used for communication and security as well as to develop software services. In the following we highlight some limitations and weaknesses of Mind Home. First, Mind Home is not provided with mechanisms to i) identify possible security attacks and ii) isolate possible misbehaving nodes. Second, security problems can be present in Mind home services since no tools to reveal software security weaknesses have been used. Third, third-party APIs are used to offer advanced functionalities such as voice control of the house. This makes user data prone to data reuse by third party companies, hence, arising privacy concerns. The system architecture of SIFIS-Home project is compatible to the one used by Mind Home. Specifically, the SIFIS-Home project takes care to produce a secure-by-design solution that is going to overcome the above-mentioned limitations of Mind Home. Mind commits to test the functionalities and features of the SIFIS-Home project extensively. Then, we are going to integrate them in the future versions of Mind Home product.

Riots Global Oy (RIO)

Riots wants to be actively involved in the development of security in IoT. As an innovative and agile SME IoT company, Riots is interested in finding out different larger scope possibilities in the field of IoT security and regards this project as a great opportunity to examine larger scale open-source solutions. As Riots views IoT security as a rising central topic in smart homes and other similar

infrastructures, the company firmly supports new and forthcoming established open-source solutions in IoT security. It is in our interest to develop and offer functioning, secure, and reliable IoT solutions for wide commercial use. Riots is especially interested in the concept and implementation of privacy within a smart building – a large entity with a vast number of smaller components and several levels of users. The challenge of secure and correct distribution of rights to access different sets of the collected data and how to ensure the integrity of the network as a whole against malicious actions is one of our main focus points. In addition to strengthening our own product security, Riots wants to be involved in creating best practices and quality standards when it comes to IoT security.

Sensative AB (SEN)

Results from the SIFIS Home project is a vital part of Sensative Yggio. It both includes the heart of Sensative Yggio which is the FIWARE compliant open-source RATATOSK publish / subscribe Context Broker which 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 as well as configuration related data needed maintain the integrity of the system. Further is the new mobile phone adapted UX of Yggio, like the Device Manager and coming Market Place, driven by the UI design and the open-source code developed in SIFIS Home. SENS also plans to add anomaly detection functionality to Yggio as part of the analytics results from WP4 in SIFIS Home.

SENS plans to actively promote all the results of the project to our customers, partners and ecosystem of service providers. This will be done both is specific meeting with partners and customer as well as in more general type 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 outcome of Research & Development (R&D) activities, it will produce know-how, specifications and software components as project results.

Expected exploitable results include: preventive and reactive cybersecurity solutions; their 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 are documented in the project Deliverables D3.2 "Preliminary report on Network and System Security Solutions", D7.1 "Preliminary Dissemination Report" and D7.2 "Preliminary 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 extension of the project.

- Dissemination of research and development results through academic publications at international journals, conferences and workshops.
- Contribution to open standardization activities, with particular reference to the IETF body.
- Integration of software components into official open-source software libraries as well as into further related R&D activities.
- Establishment and reinforcement of collaborations for joint research and dissemination activities, with Swedish and international partners from both the industry 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 comprising IT-security topics and activities.

In addition to RISE itself, the results 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 implementations, leveraging the support and efforts of open collaborative communities.

As to the "Research community", results from RISE will benefit the overall availability of findings and results on cybersecurity topics, especially in terms of accessible related works and documentation, as well as of open standards and software implementations. This will yield a more vivid and productive research community.

Centria University of Applied Sciences (CEN)

Centria University of Applied Sciences is located in three different campus areas in Ostrobothnia, Finland. Centria’s Research and Development has expertise in the fields of wireless networks and systems, positioning, cyber security 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 is 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 Cyber Security Laboratory tests and develops the security of industrial Internet and wireless systems. Centria provides

expertise in data security management to SMEs.

Centria University of Applied Sciences uses the results of SIFIS-Home for computing sciences as well as for IoT-related courses. Centria will contribute to SIFIS-Home by producing academic journals and conference proceedings. 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. The project results will also be used in preparation work for upcoming projects, where State-of-the-art knowledge is needed.

Politechnico 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. 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.

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, and collaborating in dissemination activities with national and international partners from academia and the industry.

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

5 Community building

The SIFIS-Home consortium partners have engaged into the following community building activities.

WebThings

- Participation to some meetings of the WebThings community.
- Direct discussions with the project leader Ben Francis (Krellian CEO), discussed interest about integration of SIFIS-Home security components into the WebThings framework.
- Contributed updates and fixes to the WebThings Frameworks, both the Rust and the Arduino ones.

AIxIA (Italian Association for Artificial Intelligence)

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

6 Conclusion

To conclude, the SIFIS-Home project and its preliminary results have significant implications for business opportunities of smart home security and IoT security with a high European and international market demand as both the IoT technology is becoming more widespread, and the cyber security and privacy awareness of consumers is increasing. Consequently, as IoT technology and various smart home systems are becoming more common, the attack surface increases and creates new cyber security risks. This is an issue which the customers and manufacturers might not adequately understand. This emphasizes also the need for standardized protocols that are highlighted in this report. Detailed activities of SIFIS-Home partners regarding standardization are provided in the deliverable 7.2 *Preliminary Standardization Report*.

This document has summarized the preliminary business and exploitation plans and strategies to utilize the results of the SIFIS-Home project after the project completion by analyzing the business and exploitation context according to the understanding acquired during the first half of the project. This document will be updated and obsoleted by the Deliverable D7.6 *Final Business and Exploitation* plan to be released at the end of the project.

7 Annex A: Glossary

Acronym	Definition
DDoS	Distributed Denial of Service
IoT	Internet of Things
MUD	Manufacturer Usage Description
NSSM	Not So Smart Devices
OS	Operating System
RIA	Research and Innovation Action
SIFIS-Home	Secure Interoperable Full-Stack Internet of Things for Smart Home

References

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

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

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.

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

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