D7.7

SIFIS-Home Website

WP7 – Exploitation, Dissemination and Standardization

SIFIS-HOME
Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/01/2021
Actual submission date: 27/01/2021

26/01/2021
Version 1.0

Responsible partner: CEN
Editor: Laura Palovuori
E-mail address: laura.palovuori@centria.fi

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

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

Authors: Laura Palovuori (Centria), Giacomo Giorgi (CNR), Sini Olkanen (F-Secure)

Approved by: Saila Kakko (Riots), Luca Ardito (Polito)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	20/12/2020	Defined ToC	CEN, CNR	All
0.2	13/01/2021	Hosting and Metadata	CNR	Section 1, Section 2
0.3	14/01/2021	Website structure and Social media	CEN	Section 3, Section 4
0.4	18/01/2021	Platform and Website structure and Social media	CEN	Section 2, Section 3, Section 4
0.5	18/01/2021	Ready for Review	CEN	Annex A, Annex B
0.5	22/01/2021	Included first Review	CEN	All
0.6	22/01/2021	Included Second Review	CEN	All
1.0	26/01/2021	Ready for submission	CEN	First page and Revision history and Hosting and development

SIFIS-Home aims at providing a secure-by-design and consistent software framework for improving resilience of Interconnected Smart Home Systems at all stack levels. To this end, 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 cyber-attacks and intrusion attempts or violation of user-defined policies, thus increasing control and trust of Smart Home end users.

Smart Home is an emerging application paradigm which has been gaining increasing popularity. Most recently, the Internet of Things (IoT) has been fostering a vision of Smart Home systems, where users can install connectable (smart) devices and appliances that cooperate to automatically manage home services and functionalities. This emerging market is rapidly attracting software developers to produce novel applications and services, to provide additional Smart Home functionalities. However, noticeable barriers and concerns are still present, mainly related to cyber-security and safety within Smart Home systems, as well as to the privacy and integrity of produced and consumed data, most of which are personal and sensitive. Also, many Smart Home devices use custom and proprietary security solutions that do not account for interactions with other devices in the Smart Home system. Plus, developers have to develop applications adaptable to different systems and architectures, where security aspects are often neglected or poorly addressed.

The consortium combines leading industry players in the IoT, telecommunication and cyber-security markets with research and academic institutions, also involved as key contributors to premier international standardisation bodies (e.g. IETF), and having leading roles in the SPARTA, CONCORDIA and CyberSec4Europe projects of the European Cyber Competence Network. SMEs active in the Smart Home and IoT markets and Open Source community complete the consortium.

LEGAL NOTICE

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use, which might be made, of the following information.

The views expressed in this report are those of the authors and do not necessarily reflect those of the European Commission.

Executive Summary

This document describes the SIFIS-Home website structure and reports the website’s development, security management, and hosting process. High-level descriptions of the website’s pages and their content are included, and this document also briefly describes the integration of the website with the project’s social networks.

Table of contents

1. Introduction

A website is a fundamental and necessary tool for establishing a presence on the web. For this reason, SIFIS-Home prepared and made accessible a website, starting from the second month into the project. The website aims to be a platform that offers an easy and free access to all SIFIS-Home public content, including deliverables, scientific publications, and white papers. The website presents the SIFIS-Home mission and vision, acknowledging and highlighting the European dimension. Furthermore, we strived to make the website as accessible as possible, believing in a dynamic approach where new content becomes available also through the project's social network channels which have been activated and have already been in use from the beginning of the project.

2. Hosting and Development

This section reports the technical aspects related to domain and website hosting and development.

2.1. *Domain and Address*

The SIFIS-Home project website is available at the following domain: www.sifis-home.eu . The domain name has been registered by the coordinator through the Aruba.it registrar and is set to be automatically renewed. The static IP address assigned to the domain is 146.48.96.132. The IP address is a class B IP provided by CNR which is the Italian domain registration authority.

The following sub-domains have also been prepared to host -specific project content:

www.blog.sifis-home.eu: hosts the blog with new content released monthly, intended for wider public as an information source on the SIFIS-Home consortium and community.

www.code.sifis-home.eu: redirects to the public GitHub repository hosting the code developed in the SIFIS-Home project.

Additional subdomains can be defined during the project if needed. In that case, the new subdomains are reported in deliverables D7.1 and D7.4 as part of dissemination.

2.2. *CMS and Platform*

WordPress is a practical website builder and a sturdy content management system. It is easy to use and flexible enough for creating different types of websites. WordPress can be used in various ways, and it offers thousands of free website templates (themes) that are easy to customize. It is possible to add custom functionalities to the site by using free plugins as well; WordPress plugins are like apps for the website that offer more functions, for example for analytics, etc. WordPress includes a built-in media uploader for handling images as well as audio and video files. In the SIFIS-Home project we intend to be active online. With WordPress the website can be developed flexibly when needed.

WordPress is free to download, install, use, and modify content with. Due to its wide and popular use, most problems that occur during using can be solved with the help of Google.

WordPress includes a built-in update management system which allows the user to update the plugins and themes through the WordPress admin dashboard. WordPress sends a notification when a new version is available, so users can update their website with a simple click of a button.

One of the advantages of WordPress is search engine optimization (SEO) support. WordPress is written using standard compliance high-quality code and produces semantic markup. This is an asset when it comes to visibility on Google and other search engines.

In order for the website to be ranked in search engines, a SEO plugin has been added on the website. The chosen plugin, *Yoast SEO,* is a known and widely used WordPress plugin for this purpose because it helps the website content to meet the high SEO standards and increases overall readability.

In SIFIS-Home security is in the centre of everything we do, and WordPress is considered a safe and secure platform for running a website. To protect the data from any accidents or hacking, using a backup plugin to automatically create backups and store them safely is easy.

2.3. Hosting

The SIFIS-Home website is hosted on a dedicated Virtual Machine (VM) on the CNR website. The VM is installed on a server that has the characteristics reported in Table 1.

Table 1: Current system hosting the website.

Component	Characteristics
Processor	Proliant DL385P Gen 8 16 CPU x 2.496 GHz
Processor Type	AMD Opteron 6380
Memory	31.95 GB
Datastore	2 x 2.73 TB

Using a VM to host the website holds advantages in terms of management, such as the ease of moving the VM between servers or create a backup of the whole VM in one go.

The VM was created to meet requirements for running WordPress 5.6. Table 2 shows the WordPress requirements and the VM characteristics adopted.

Table 2: System requirements.

Component	WordPress 5.6 requirements	VM characteristic
Disk Space	1 GB+	100 GB
Web Server	Apache or Nginx	Apache
Database	MySQL version 5.6 or greater or any version of MariaDB 10.1 or greater	MySQL version 8.0.22
RAM	512 MB+	8 GB
PHP	Version 7.4 or greater	Version 7.4.3
Processor	1.0 GHz+	8 CPU x 2.493 GHz
Operating System	Not specified	Ubuntu 20.04.1 LTS (64bit)

This alternative meets the minimum requirements for running WordPress 5.6 with good performance and provides a wide margin for storage space requirements.

2.4. *Security Management*

A hacked site can cause severe damage that can affect user privacy or the reputation of the project. Several types of website attacks are generally known and can have negative consequences. In our case, hackers can steal information from the registered users or passwords, install malicious software, delete website’s data, launch a Denial of Service (DoS) attack that causes website downtime, or publish false information causing reputation damage to the project. For these reasons security management of the website and the hosting resources is needed. The following paragraphs describe actions introduced to minimize the risk of an attack.

2.4.1. Operating System

The first security choice adopted for the hosting VM is related to the Operating System (OS). Although hacking risks exist for Windows and Linux OS, Windows is generally more vulnerable to threats. In contrast, Linux provides fewer malware opportunities for hackers to exploit. In addition, Linux is more stable and hardly ever needs a reboot. Despite all this, much will depend on keeping the software up-to-date and the server properly configured. In the following are described all the settings applied.

2.4.2. SSH Connection

Secure file transfer to and from the VM is an important facet of website security in the hosting environment. Encryption ensures that any data sent is not visible to an attacker sniffing the network traffic.

Secure Socket Shell (SSH) is a secure network protocol and widely used way of safely administering remote servers. With SSH any kind of authentication, including password authentication and file transfers, is completely encrypted. This protocol is adopted in the hosting VM, making it accessible only with SSH public-key authentication with RSA algorithm keys.

2.4.3. Firewall

An additional level of security is given by the introduction of the firewall on the hosting VM. The aim is to allow, restrict, and filter access to the system. Access to the VM is allowed only from the CNR subnet while only the Apache port is opened to publish the website.

2.4.4. Backup

Maintaining backups of the WordPress site is one of the most important recurring tasks to improve security. A good set of backups can save the website when absolutely everything else has gone wrong. Suppose a malicious attacker decides to wipe all the site files or corrupt them with buggy scripts – the damage can be undone by restoring the site from the backups. For this purpose, a plugin called *UpdraftPlus Backup/Restore* was installed in WordPress; it is a widely used scheduled backup plugin. An automatic fortnightly backup is set to store the database and the website files directly on Google Drive storage.

2.4.5. Updates

OS, software installed on the hosted VM, plugins, and themes can become deprecated, obsolete, or include vulnerabilities that pose serious security risks to hosting VM and the website. A regular audit of VM software, plugins, themes, and updates has to be programmed to improve security. The actions reported in Table 3 are scheduled to be manually performed every month.

Table 3: Monthly security review process.

Action	Description
Updating VM software	Software updates are important because they often include critical patches to security holes. We see many of the more harmful malware attacks take advantage of software vulnerabilities in common applications, like operating systems and browsers.
Removing unused plugins and themes	Storing unwanted plugins in WordPress installation increases the chance of a compromise, even if they are disabled and not actively being used in the current installation.
Updating WordPress	When a new version of WordPress comes out, its installation is recommended. Before the update the following actions are needed: • Create a backup version of the website. • Review the release notes to identify if changes will have any negative impact on the website. • Test the update on a development site to verify that the themes, plugins, and other extensions are compatible with the latest version.

3. Website Structure

The website structure is designed according to the project´s need. On the SIFIS-Home project website we want the visitors to find everything they want quickly and easily. The home page presents a summary of the project and the **News** page displays the latest posts and other content. The **Publications** page presents scientific points of view. During the project's duration we can add new pages and functionalities if necessary.

Home is the home page, where the visitor can see the name and the description of the project (Figure 1. and Figure 2.).

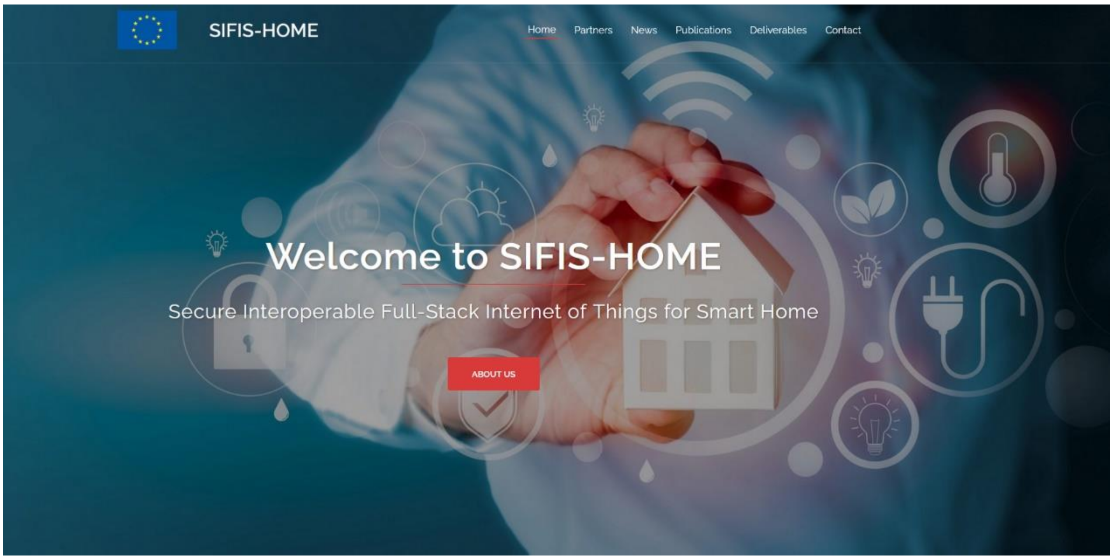
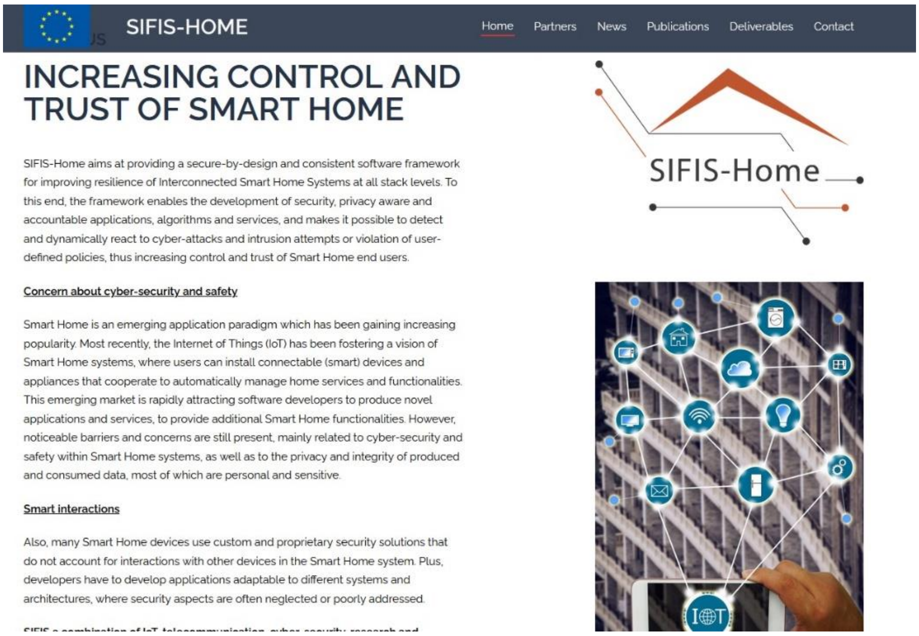


Figure 1. The Home page, URL http://www.sifis-home.eu lands here.



INCREASING CONTROL AND TRUST OF SMART HOME

SIFIS-Home aims at providing a secure-by-design and consistent software framework for improving resilience of Interconnected Smart Home Systems at all stack levels. To this end, 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 cyber-attacks and intrusion attempts or violation of user-defined policies, thus increasing control and trust of Smart Home end users.

Concern about cyber-security and safety

Smart Home is an emerging application paradigm which has been gaining increasing popularity. Most recently, the Internet of Things (IoT) has been fostering a vision of Smart Home systems, where users can install connectable (smart) devices and appliances that cooperate to automatically manage home services and functionalities. This emerging market is rapidly attracting software developers to produce novel applications and services, to provide additional Smart Home functionalities. However, noticeable barriers and concerns are still present, mainly related to cyber-security and safety within Smart Home systems, as well as to the privacy and integrity of produced and consumed data, most of which are personal and sensitive.

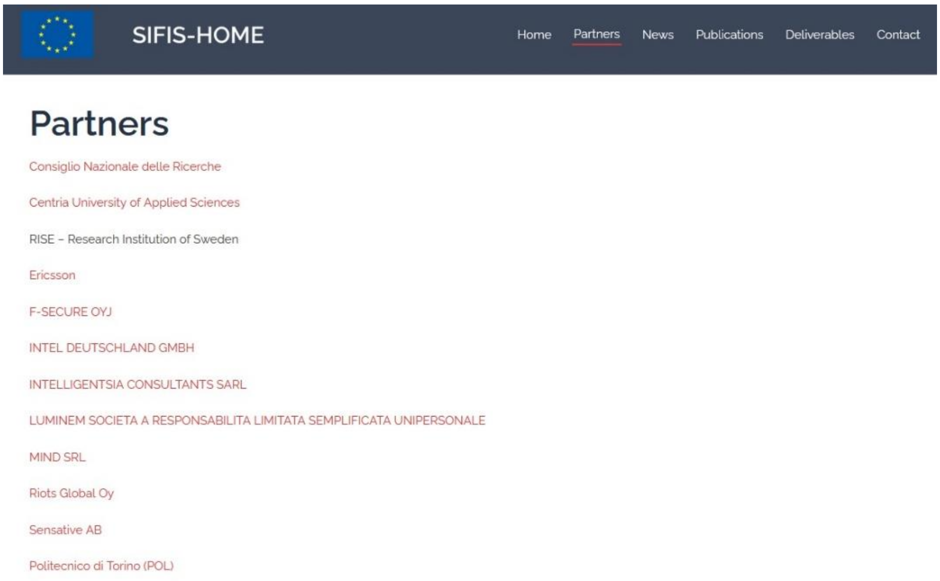
Smart interactions

Also, many Smart Home devices use custom and proprietary security solutions that do not account for interactions with other devices in the Smart Home system. Plus, developers have to develop applications adaptable to different systems and architectures, where security aspects are often neglected or poorly addressed.

SIFIS a combination of IoT, telecommunication, cyber-security, research and

Figure 2. A visitor can read the description of the project after scrolling down the Home page.

On the **Partners** page the visitor can find all the project partners. At the beginning there is a list of partners. By clicking any of these list items the visitor can jump directly to a presentation of all the partners. Along the partner presentations the visitor can see the partners' logos and links to their websites (Figure 3. and Figure 4.).



Partners

Consiglio Nazionale delle Ricerche

Centria University of Applied Sciences

RISE – Research Institution of Sweden

Ericsson

F-SECURE OYJ

INTEL DEUTSCHLAND GMBH

INTELLIGENTSIA CONSULTANTS SARL

LUMINEM SOCIETA A RESPONSABILITA LIMITATA SEMPLIFICATA UNIPERSONALE

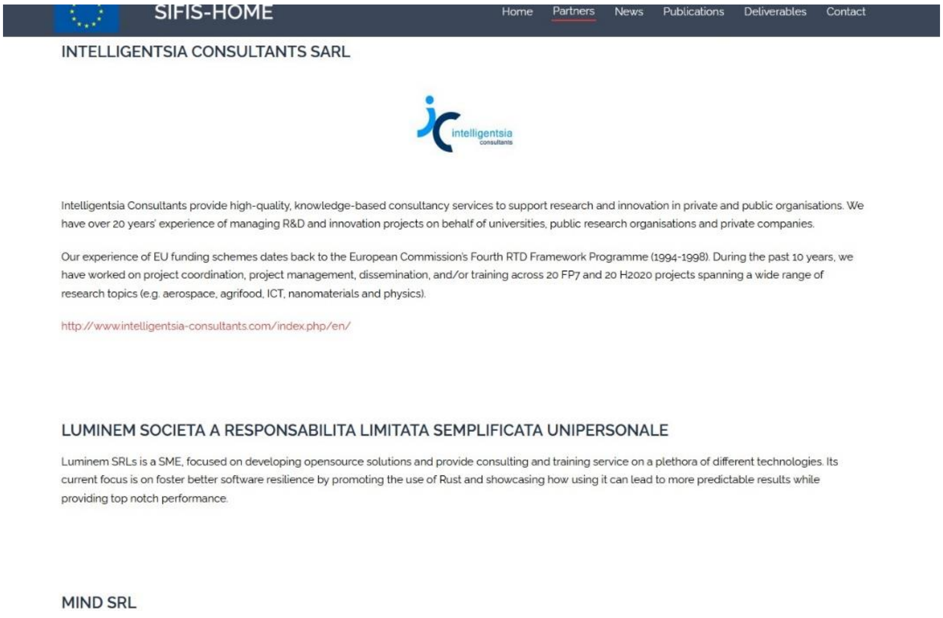
MIND SRL

Riots Global Oy

Sensative AB

Politecnico di Torino (POL)

Figure 3. The Partners page displays a list of all the partners. The headers in red are links to the descriptions of each partner.



INTELLIGENTSIA CONSULTANTS SARL

Intelligentsia Consultants provide high-quality, knowledge-based consultancy services to support research and innovation in private and public organisations. We have over 20 years' experience of managing R&D and innovation projects on behalf of universities, public research organisations and private companies.

Our experience of EU funding schemes dates back to the European Commission's Fourth RTD Framework Programme (1994-1998). During the past 10 years, we have worked on project coordination, project management, dissemination, and/or training across 20 FP7 and 20 H2020 projects spanning a wide range of research topics (e.g. aerospace, agrifood, ICT, nanomaterials and physics).

http://www.intelligentsia-consultants.com/index.php/en/

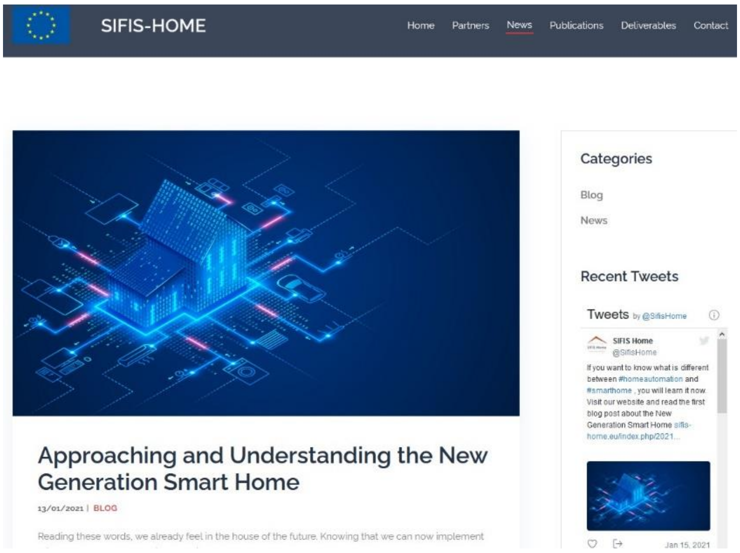
LUMINEM SOCIETA A RESPONSABILITA LIMITATA SEMPLIFICATA UNIPERSONALE

Luminem SRLs is a SME, focused on developing opensource solutions and provide consulting and training service on a plethora of different technologies. Its current focus is on foster better software resilience by promoting the use of Rust and showcasing how using it can lead to more predictable results while providing top notch performance.

MIND SRL

Figure 4. This is an excerpt from the Partners page with names, logos, and links to the website of each partner.

News contains all the news, blog posts, and articles in chronological order. Everything is categorized, so the visitor can easily find the desired content. The aim is to produce text and content that is understandable and arouses interest in the project in the eyes of big audiences as well as within the IoT community. Here the visitors can also follow the latest Tweets. We can add images, audio, and video files (Figure 5.) on the page as well.



Approaching and Understanding the New Generation Smart Home

13/01/2021 | BLOG

Reading these words, we already feel in the house of the future. Knowing that we can now implement

Tweets by @SifisHome

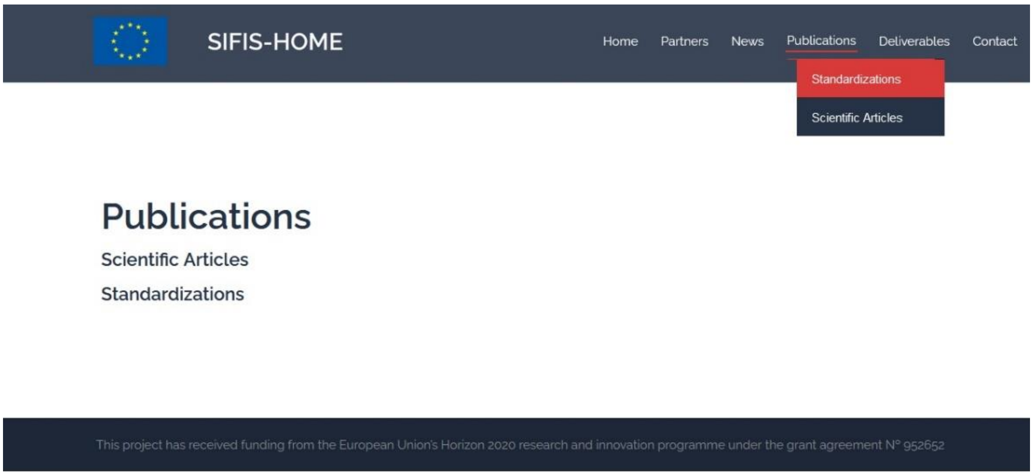
SIFIS Home
@SifisHome

If you want to know what is different between #homeautomation and #smarthome , you will learn it now. Visit our website and read the first blog post about the New Generation Smart Home sifis-home.eu/index.php/2021...

Jan 15, 2021

Figure 5. Excerpt from the News page with a blog post. Categories help the visitor to navigate. Recent Tweets can be followed here too.

The **Publications** page (Figure 6.) introduces two topics: **Scientific articles,** a list of articles and links to publications, and **Standardizations** which contains the work done in the project (Figure 7.). More topics like Scientific articles and Standardization can be added if needed. The **Deliverables** page will contain a full list of all the deliverables produced during this project as well as links to the deliverable documents. **Contact** refers to the project coordinator in Italy: Italian National Research Council (CNR) - Consiglio Nazionale delle Ricerche.



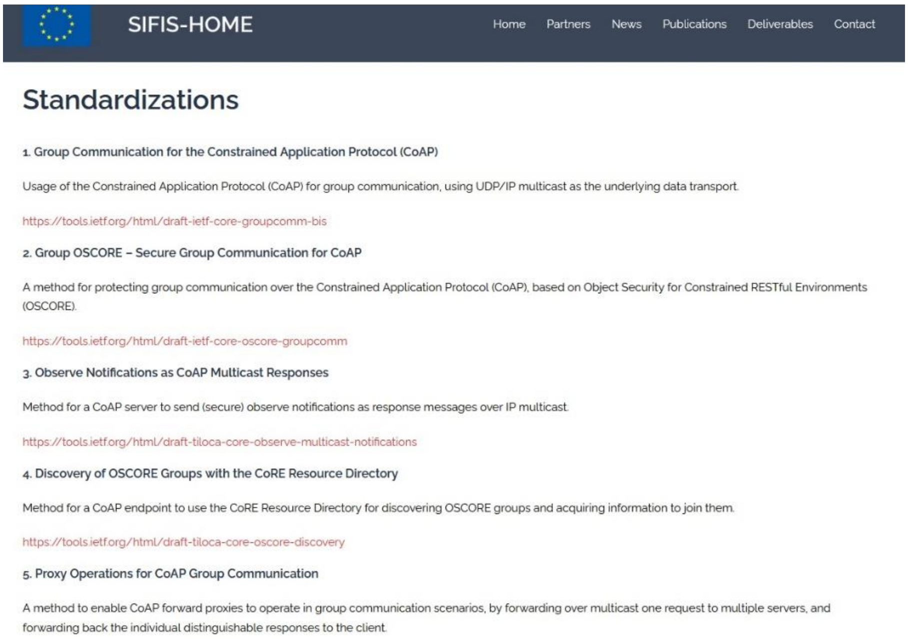
Publications

Scientific Articles

Standardizations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement N° 952652

Figure 6. Under Publications there are two sub-pages, Standardizations and Scientific Articles.



Standardizations

1. Group Communication for the Constrained Application Protocol (CoAP)

Usage of the Constrained Application Protocol (CoAP) for group communication, using UDP/IP multicast as the underlying data transport.

https://tools.ietf.org/html/draft-ietf-core-groupcomm-bis

2. Group OSCORE – Secure Group Communication for CoAP

A method for protecting group communication over the Constrained Application Protocol (CoAP), based on Object Security for Constrained RESTful Environments (OSCORE).

https://tools.ietf.org/html/draft-ietf-core-oscore-groupcomm

3. Observe Notifications as CoAP Multicast Responses

Method for a CoAP server to send (secure) observe notifications as response messages over IP multicast.

https://tools.ietf.org/html/draft-tiloca-core-observe-multicast-notifications

4. Discovery of OSCORE Groups with the CoRE Resource Directory

Method for a CoAP endpoint to use the CoRE Resource Directory for discovering OSCORE groups and acquiring information to join them.

https://tools.ietf.org/html/draft-tiloca-core-oscore-discovery

5. Proxy Operations for CoAP Group Communication

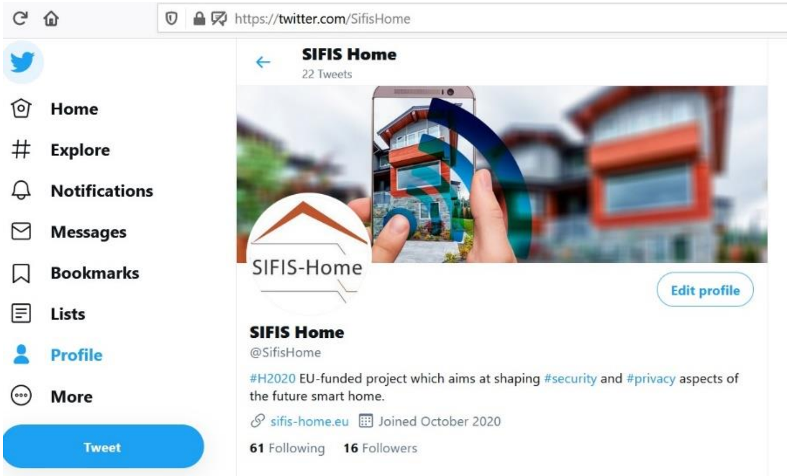
A method to enable CoAP forward proxies to operate in group communication scenarios, by forwarding over multicast one request to multiple servers, and forwarding back the individual distinguishable responses to the client.

Figure 7. This section lists the activities related to standardization done in the project.

4. Integration with Social Channels

Social media channels are a practical way to draw visitors to the project website. The project created a Twitter account (Figure 8.), a LinkedIn account, and a YouTube channel so that people all over the world can find SIFIS-Home easily. Twitter and LinkedIn are also practical tools for following other projects and the latest news about smart homes, IoT, and cyber security.

Videos published on YouTube give the project visibility and create interest in the eyes of wide audiences, and YouTube videos are easy to share on the website. Tweets are visible also on the website under **News**.



SIFIS Home
22 Tweets

SIFIS Home
@SifisHome

#H2020 EU-funded project which aims at shaping #security and #privacy aspects of the future smart home.

sifis-home.eu Joined October 2020

61 Following 16 Followers

Figure 8. A screenshot of the SIFIS-Home Twitter profile 18th January 2021.

5. Conclusion

A website is essential in web presence, and social media is a way to invite people to visit the website. An interesting website can lead the audience to follow our social media channels.

The website makes taking part in the SIFIS-Home project easy for big audiences. We will share on the website scientific articles, standardizations, events, and videos. We will also publish interesting blog posts as we consider it a potential and useful tool for popularizing complicated concepts like IoT and the smart home, and we want the idea of New Secure Interoperable Full-Stack Internet of Things for Smart Home to be accessible to big audiences. Usually blog posts collect great visibility in social media as well.

We wanted to create a flexible website, and that is why we chose WordPress as a platform. Creating and updating websites with WordPress is easy, and it allows us to create new pages and add functionalities effectively on the website during the project if needed.

The SIFIS-Home project website is available at the following domain: www.sifis-home.eu. The website is hosted on a dedicated VM on the CNR website. On the website's security management point of view we take into account the operating system, SSH connection, firewall, backups, and updates.

6. Annex A: Glossary

Acronym	Definition
SIFIS-HOME	Secure Interoperable Full-Stack Internet of Things for Smart Home
VM	Virtual Machine
OS	Operating System
DoS	Denial of Service
SSH	Secure Socket Shell
SEO	Search Engine Optimization
RAM	Random Access Memory
CPU	Central Processing Unit
PHP	General Purpose scripting language for web development
GB+	Gigabyte or more
MB+	Megabyte ore more

7. Annex B: Links

Link	Description
https://www.sifis-home.eu	The SIFIS-Home project website
https://sifis-home.eu/wp-admin	The WordPress administrator page to change settings and publish new contents (Restricted access).
https://www.sifis-home.eu/index.php/category/blog/	The blog of SIFIS-Home, accessible from the website.
https://twitter.com/SifisHome	Twitter Page for the SIFIS-Home project (Tweets integrated in the website).