D1.2

Final Architecture Requirements Report

WP1 – Distributed System Architecture

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 30/09/2021
Actual submission date: 30/09/2021

Responsible partner: FSEC
Editor: Marko Komssi;
E-mail address: marko.komssi@f-secure.com

24/09/2021
Version 1.1

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: Riccardo Coppola (POL), Luca Ardito (POL), Andrea Saracino (CNR), Giacomo Giorgi (CNR), Wisam Abbasi (CNR), Domenico De Guglielmo (MIND), Marko Komssi (FSEC)

Approved by: Marco Tiloca (RISE)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	19/05/2021	Defined ToC	FSEC, CNR, POL	All
0.2	12/06/2021	Refinement of contents from D1.1	POL	All
0.3	18/07/2021	New requirements and feedback from WP3 and WP4	FSEC, CNR, POL	Section 4, 5
0.4	31/07/2021	Requirement validation	FSEC, CNR, POL	Section 6
1.0	12/08/2021	Ready for review	FSEC, CNR, POL	All
1.1	24/09/2021	Ready to submit	FSEC, CNR, POL	All

Executive Summary

The main objective of the SIFIS-Home project is to provide a secure-by-design and consistent software framework for improving resilience of interconnected smart home systems at all stack levels. In order to address this goal, the software framework shall ensure correct functionality of the smart home system as well as enforce security, privacy and safety of all SIFIS-Home users. This calls for eliciting both functional and non-functional requirements, with a special focus on security and privacy aspects alongside the functionality of the smart home architecture.

This deliverable is the final report documenting the architecture requirements for the SIFIS-Home framework. The deliverable is an update to D1.1 "Initial Architecture Requirements Report", as it extends and finalizes the initial set of functional and non-functional requirements, based on input and feedback received from WP3 and WP4 through the respective deliverables D3.1 and D4.1. This deliverable does not report only the revised requirements from D1.1, but it also describes the process used for eliciting and defining those requirements. In addition, it presents the method that will be used to formally evaluate and validate the collected requirements during the development progress.

The final set of requirements have a significant role in the SIFIS-Home project. They will be taken as guidelines in WP3 and WP4, as well as validated and further refined within the activities of WP5 and WP6 at later stages in the project.

Table of contents

1 Introduction

The SIFIS-Home project aims at providing a *software framework* that facilitates the management of security in smart home environments, ensuring certifiable levels of privacy and resilience in smart home applications and systems. As illustrated in Figure 1, this is achieved by leveraging two main components:

i. A software framework utilising secure IoT specific communication protocols that enables:

   a. securely managing and enforcing security functionalities,

   b. performing privacy-aware data handling, aggregation and analysis,

   c. ensuring secure communication in a resilient, easy and efficient way.

ii. A development toolkit that allows (third party) developers to provide applications that exploit the potential of the SIFIS-Home Security Architecture, to integrate security functionalities in their applications.

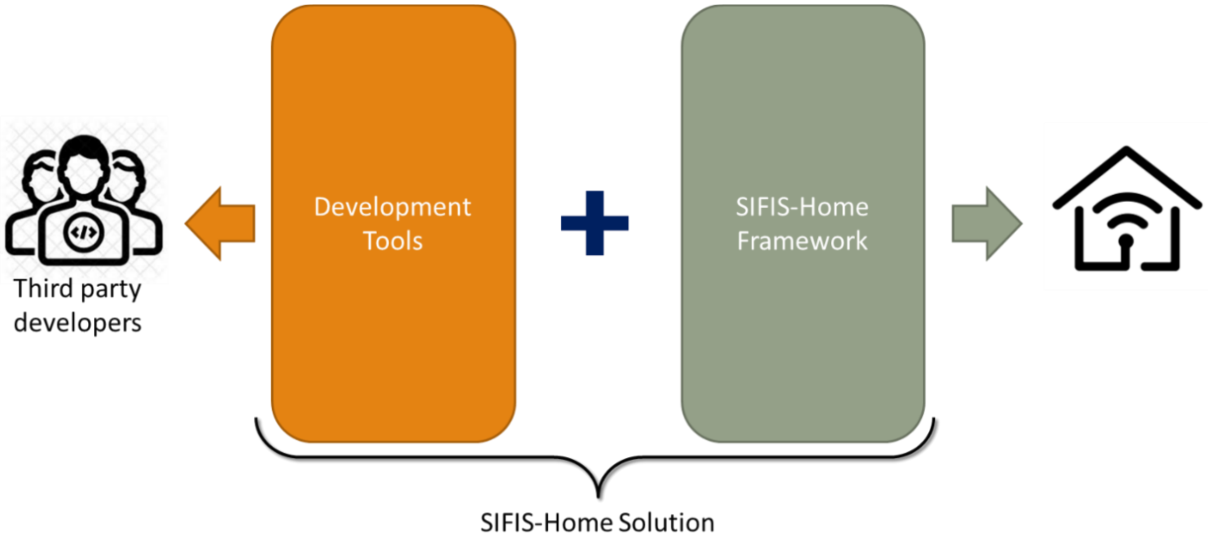


Figure 1: SIFIS-Home main building blocks

The SIFIS-Home software framework is devoted to ensure correct functionality of the smart home system. The framework must enforce the security of connected devices as well as the privacy and safety of home tenants. To this end, the framework must be designed considering a great range of functional, technical and security requirements, reflecting the needs for a flexible, performing, resilient, configurable and privacy aware smart home framework.

This deliverable reports the finalized set of requirements for the SIFIS-Home framework, both Functional and Non-Functional. The set of requirements has been revised and extended, based on the input and feedback received from WP3 and WP4 through the respective deliverables D3.1 and D4.1, to ensure that the requirements match the technological needs of both WP3 and WP4. This deliverable provides input to D1.3 and D1.4 for the architecture design, and to D5.1 concerning the actual implementation of the SIFIS-Home architecture and its deployment in a dedicated testbed.

The deliverable is organized as follows. Section 2 presents the incremental process of eliciting and defining requirements, while Section 3 reports the context diagram of the SIFIS-Home system. Section 4 presents the SIFIS-Home use cases, and Section 5 reports the revised requirements. Section 6 introduces a method to evaluate and validate the requirements and Section 7 concludes the deliverable.

2 Process of eliciting and defining requirements

The process of eliciting and defining requirements was incremental. Following a bottom-up approach [Crespi, 2008] in D1.1, the use cases were taken as a starting point and the initial requirements were formulated. WP1 also defined a research methodology to formalize the work. The initial requirements and the research methodology were introduced in D1.1.

This deliverable, D1.2, extends and finalizes the initial set of functional and non-functional requirements, based on input and feedback received from WP3 and WP4 through the respective deliverables D3.1 and D4.1. Figure 2 illustrates and summarized the incremental steps to elicit and define the final requirements. The initial requirements (specified in D1.1) were analysed in WP3 and WP4. Both Work Packages provided suggestions for clarifying and revising the initial requirements together with new additional requirements to be considered for inclusion. These were reported in D3.1 and D4.1, respectively. The suggestions were merged and evaluated in a series of meetings. The following step enabled each partner to provide additional suggestions on the requirements, based on both the new insights from D3.1 and D4.1 as well as additional knowledge gained during the steps of evaluation and partner analysis.

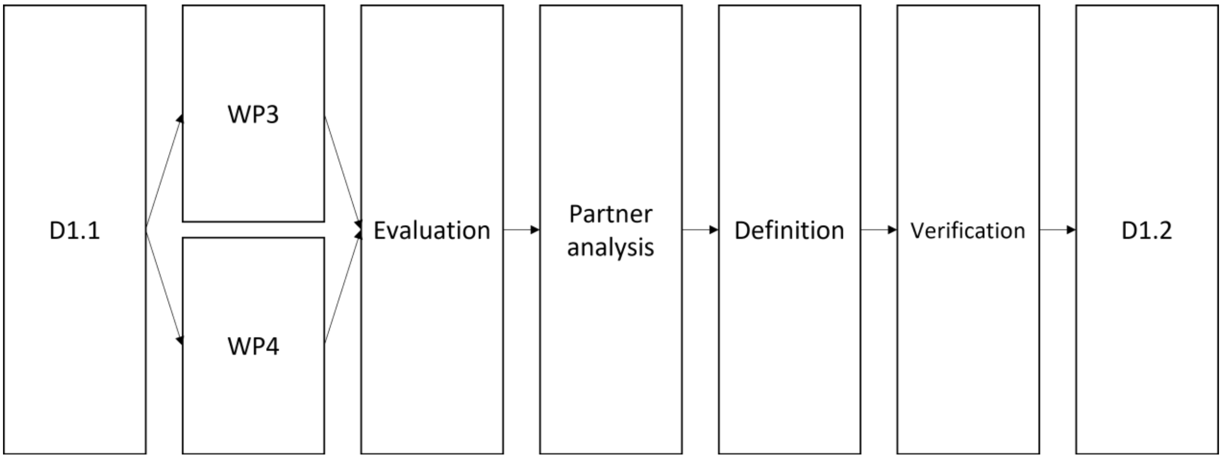


Figure 2: Steps to illustrate the process of eliciting and defining the final requirements

In the definition and verification phases, all the suggestions were re-analysed and new requirements were defined or modified accordingly. This step included collaboration and verification between partners as some of the suggestions were addressing the same requirements from multiple viewpoints. The feedback for each requirement was categorized as “OK”, “Refine”, or “Amend”. The corresponding Feedback column was added to the table of the requirements to include the definition.

These steps do not include the validation phase. It will be carried out in the activities of WP5 and WP6. Section 6 of this deliverable merely introduces a method to validate the requirements specified in the deliverable.

3 SIFIS-Home Context Diagram

Figure 3 reports the Context Diagram of the SIFIS-Home system. In the Context Diagram, we have divided the actors interacting with the system in three categories:

- **Internal entities:** Identifies a category of internal devices (i.e., located inside the home network) connected to the SIFIS-Home system.
- **External entities:** Identifies a category of external entities (e.g., devices or services) located outside the home network.
- **Users:** identifies a category of human users of the SIFIS-Home system, e.g. a utiliser of the smart devices in the SIFIS-Home network.

Detailed definitions of each category of actors are reported in the following subsections.

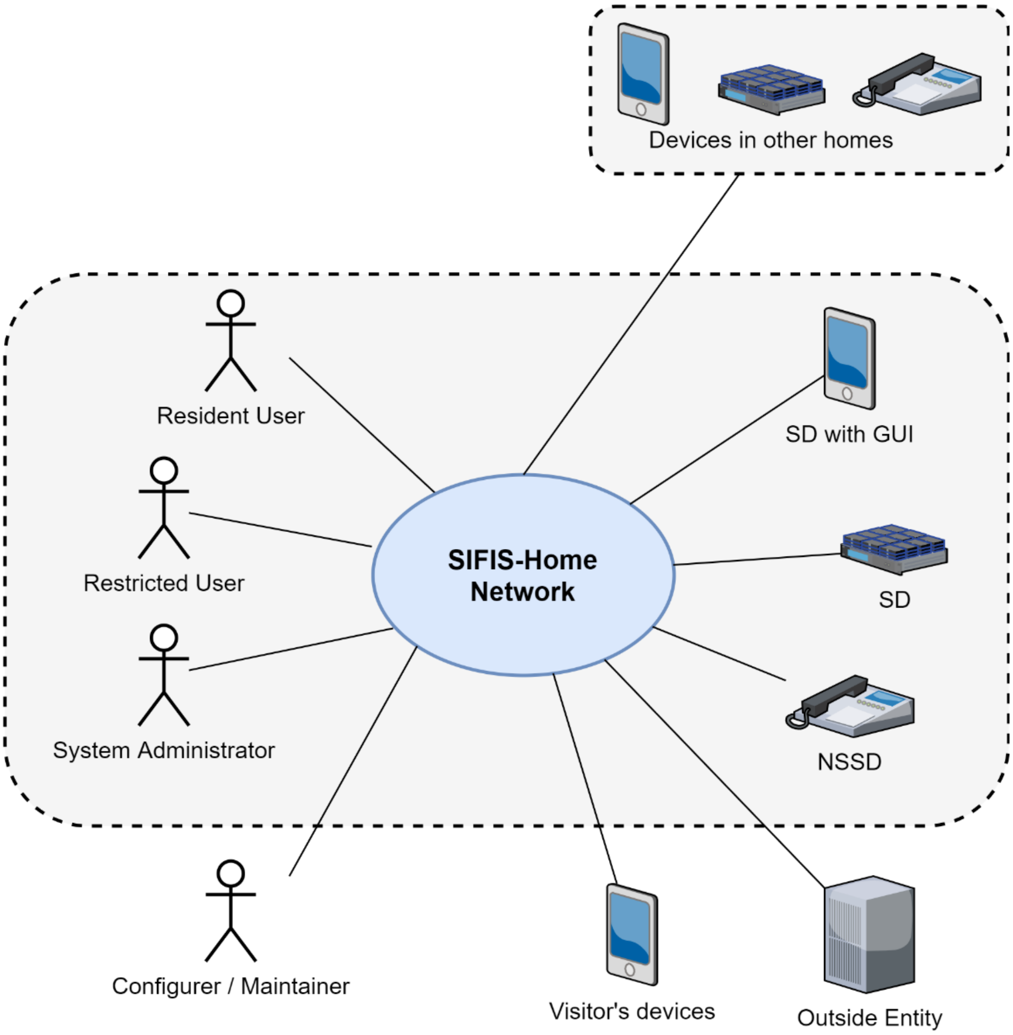


Figure 3. SIFIS-Home Context Diagram

3.1 *Internal Entities*

Table 1 reports the categories of internal entities defined for the interaction with the SIFIS-Home system. For each entity, we report the possible physical and logical interfaces through which the entity is expected to communicate within the system and network. Definitions, examples and possible variations inside a specific category of entity are reported in the following:

- **Smart Device without local GUI (Graphical User Interface):** device with good computation capabilities, with a general-purpose OS, where it is possible to install applications, and that should provide communication to the outside through an Internet connection. Examples of devices in this category include Raspberry Pie devices, smart fridges, parked cars that can be controlled.
- **Smart Device with local GUI:** smart device with local GUIs exposed to the user. Examples of devices in this category include smartphones and smart TVs.
- **Not So Smart Device (NSSD):** device with connection capabilities but with low computational power and without the possibility of installing a general-purpose OS. Examples of devices in this category include smart light bulbs, thermovalves, smart cameras, ESP 32-based devices, sensors, actuators.

Entity Type	Physical Interfaces	Logical interface
Smart Device without local GUI	WiFi connection, Ethernet, Bluetooth connection, IEEE 802.15.4, WiFi ad-hoc, IoT protocols, 5G (lowpan)	Software APIs
Smart Device with local GUI	WiFi connection, Ethernet, Bluetooth connection, IEEE 802.15.4, WiFi ad-hoc, IoT protocols, 5G (lowpan)	Software APIs
Not So Smart Device (NSSD)	WiFi connection, Bluetooth connection, IEEE 802.15.4, WiFi ad-hoc, IoT protocols, 5G (lowpan)	Software APIs

Table 1. Internal entities in the SIFIS-Home Context Diagram

3.2 *External Entities*

Table 2 reports the categories of external entities that we have defined for the interaction with the SIFIS-Home system. For each entity we report the possible physical and logical interface through which the entity is expected to communicate within the system and network. Definitions, examples and possible variations inside a specific category of entity are reported in the following:

- **Visitor's device:** a smart device of a guest who is visiting a SIFIS-Home-served smart home. Its characteristics are equivalent to the smart device with local GUI category of internal devices.
- **Outside entity:** an external entity that can interact with the SIFIS-Home system. Examples of entities in this category include cloud applications, external storages or services, services or devices that need a connection to the SIFIS-Home System (e.g., cloud based smart speaker).
- **Devices in other homes served by SIFIS-Home:** a device located in another smart home where another instance of the SIFIS-Home system is running. It can belong to any category of internal devices.

Entity Type	Physical Interface	Logical interface
Visitor's device	WiFi connection, Ethernet, Bluetooth connection, IEEE 802.15.4, WiFi ad-hoc, IoT protocols, 5G (lowpan)	GUI guest interface to the SIFIS-Home system
Outside entity	Internet connection	APIs with privacy policies
Devices in other homes served by SIFIS	Internet connection	APIs with privacy policies

Table 2. External entities in the SIFIS-Home context diagram

3.3 *Users*

In this section, we report the users of the SIFIS-Home system as part of the requirements elicitation process, to determine all SIFIS-Home stakeholders [Sharp, 1999]. In subsection 3.3.1, we report the User Categories. In subsection 3.3.2, we report the User Training for SIFIS-Home System.

3.3.1 Users Categories

Table 3 reports the categories of users that we have defined for the SIFIS-Home system. For each user, we report the possible physical and logical interface through which the entity is expected to communicate within the system and network. Definitions, examples and possible variations are reported in the following:

- **Resident user / Smart Home Resident:** A resident living in the smart home and eligible to use all the functionalities of the smart home system, and possesses the required permissions and authorizations. Resident Users can configure their own profiles and install dedicated applications, but they do not have control over the security policies in the home.
- **Restricted user:** User with restricted features according to the profiles defined in the current SIFIS-Home configuration. Examples of restricted users are visitor users, who are temporarily visiting the home and can use the digital services of the home (apartment) connected to the network; children and elderly people, who can have extensive restrictions on what they can access due to security and safety reasons.
- **System administrator:** Admin is the owner of the smart home and is responsible for managing the household’s information and communication security. There can be more than one admin per household. Each admin configures security policies and has the rights to register and unregister devices in the smart home.
- **Configurer / Maintainer:** A service provider who offers maintenance services for the building itself or for a certain part of the system (e.g., the heating system, the ventilation system, access control & security services on the premises, etc.). Their responsibilities may include ensuring specific device or functionality operability. They may not need to access all the user’s personal information stored in the system, but they need selective access to specific parts of the system, for example to perform specific device maintenance.

User	Physical Interface	Logical Interface
Resident User	Smart Device with GUI SIFIS-Home applications, which connect to FIWARE NGSI, open API on the SIFIS-Home compliant middleware	Compliant and non-compliant apps + haptic, voice commands

Restricted user	NSSD, buttons, physical interfaces in the SIFIS-compliant smart home	Haptic, voice commands, etc.
System Administrator	Smart Device with GUI or Web-Based Interface	Configuration panel of the GUI
Configurer / Maintainer	Web-Based Interface	Configuration panel of the GUI

Table 3. Categorized list of users for the SIFIS-Home system

A more complete categorization of users and other SIFIS-Home actors is reported in D1.3.

3.3.2 User Training

An important step for successful implementation is the user training, in order to help users manage and operate the system in an efficient way. The training method used in SIFIS-Home is self-instruction method, in which a training material is developed and delivered to the end user. This training material includes operating manuals and online tutorials explaining systems' functionalities, modules, and technology setup. Training material also gives instructions on how to download needed applications, setting up user accounts and profiles, permissions assignment, and how to perform some basic usecases.

4 SIFIS-Home Use Cases

In this section, we report the use case elicitation process for the SIFIS-Home system that was presented in deliverable D1.1 following the methodologies defined in [Cockburn, 1998]. In subsection 4.1, we report the User Stories for the human users defined in the Context Diagram shown in Figure 3. In subsection 4.2, we report the Use Cases derived from the Stories, each detailed with a Use case Narrative.

4.1 *User Stories*

Seven main User Stories have been defined and detailed in the following subsections for the human users of the SIFIS-Home system describing the framework functionality [Cohn, 2004]. For each User Story, we use Leffingwell's template [Leffingwell, 11], in the form *As a <actor>, I want <action>, so that <business value>*. We also report additional details about the actions in the User Story, the main actors involved, and the acceptance test that should be performed to verify and validate the story.

4.1.1 SIFIS-US-01: Smart home handling through voice command

As a

Smart home resident

I want to

use voice commands

So that

the system recognises me, provides me with services and does not share private information from my requests with external entities unless otherwise allowed.

Discussion

The smart home residents can exploit the speech recognition system offered by the SIFIS-Home framework to authenticate to the smart home. After the authentication, the resident can access home devices according to what is specified in the pertaining access and usage policies, and accordingly manage the smart devices through vocal commands expressed in natural language (e.g., turn on the light, turn down the volume). Every vocal command recorded by the system will be anonymised and maintained private to preserve the residents' privacy.

Main actors:

- Smart home resident, restricted user, smart home administrator

Acceptance test:

- The actor can authenticate to the SIFIS-Home framework using their voice.
- The actor can manage the smart home components through voice commands.
- The speech recognition engine can maintain the privacy of any sensitive information.

Storyboard (Figure 4):

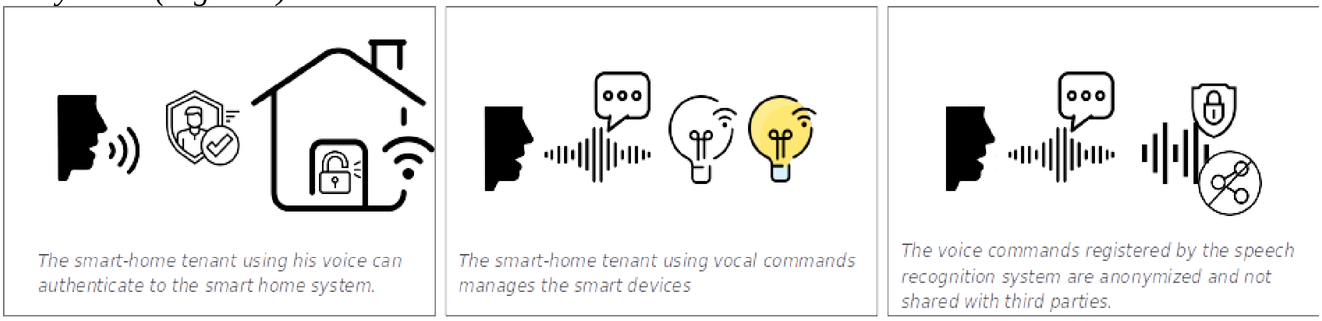

The smart-home tenant using his voice can authenticate to the smart home system.
The smart-home tenant using vocal commands manages the smart devices
The voice commands registered by the speech recognition system are anonymized and not shared with third parties.

Figure 4. A storyboard of Smart home resident to use voice commands

4.1.2 SIFIS-US-02: Smart home configuration panel

As a

Smart home administrator

I want to

have a configuration panel

So that

I can set home usage as well as security and privacy policies to protect myself, the residents and guests; and I can visualize the smart home statistics.

Discussion

The smart home administrator can access to a smart home configuration panel through which it is possible to define:

- High-level policies expressible in natural language (e.g., “Do not record sound in the living room tonight”). Those policies will trigger a reconfiguration of all the IoT devices to comply with this rule. They will be translated in a device configuration, which can limit the features of an IoT device, or inhibit the operation of a non-reconfigurable device.
- Device configurations which express how they will work in the smart environment.
- Visualize the statistics and the analytic results related to the smart home operation (e.g., energy consumptions, devices status).

The administrator will be able to define policy and device configuration in a remote way through the smart-home configuration panel offered by the SIFIS-Home framework.

Main actors:

Smart home administrator

Acceptance test:

- The smart home administrator can remotely set security and privacy policies defining how each smart home user can access and use the home devices.
- The smart home administrator can remotely set the configuration of each home device.
- The smart home administrator can visualize the smart-home statistics.

Storyboard (Figure 5):

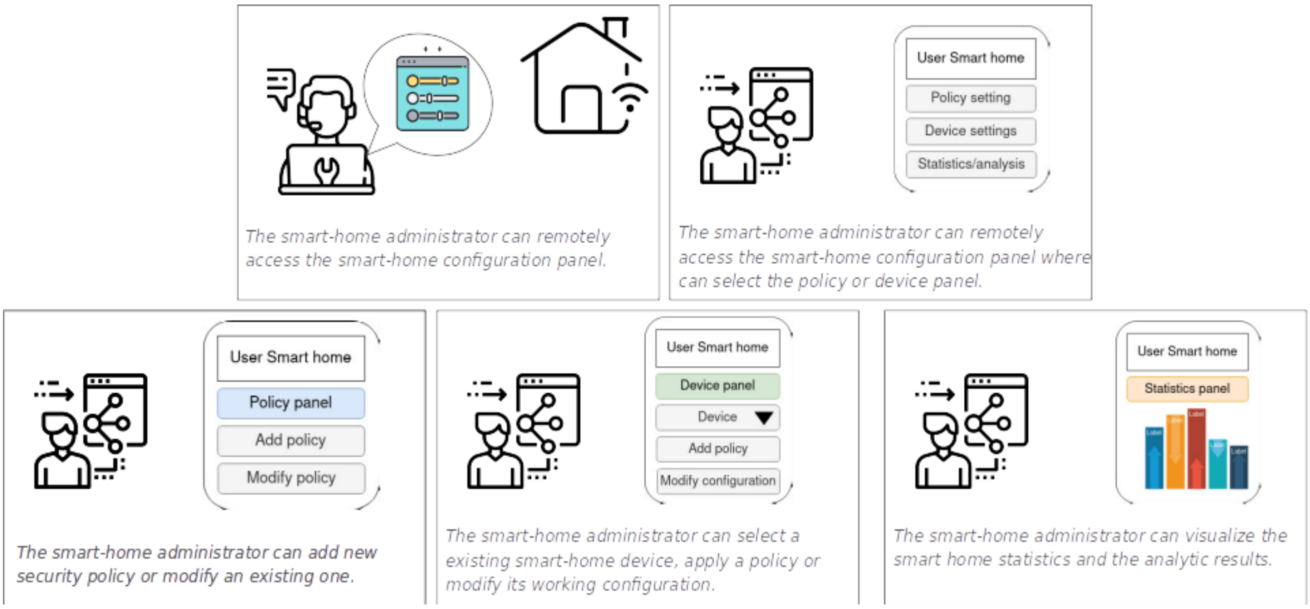

The smart-home administrator can remotely access the smart-home configuration panel.
User Smart home
Policy setting
Device settings
Statistics/analysis
The smart-home administrator can remotely access the smart-home configuration panel where can select the policy or device panel.
User Smart home
Policy panel
Add policy
Modify policy
The smart-home administrator can add new security policy or modify an existing one.
User Smart home
Device panel
Device
Add policy
Modify configuration
The smart-home administrator can select a existing smart-home device, apply a policy or modify its working configuration.
User Smart home
Statistics panel
The smart-home administrator can visualize the smart home statistics and the analytic results.

Figure 5. A storyboard of Smart home administrator to have a control panel

4.1.3 SIFIS-US-03: Physical anomaly detection in the smart home

As a

Smart home resident/administrator

I want to

be notified if someone enters my home without permission or if an anomalous event occurs

So that

I can protect myself and ask for help from the authorities.

Discussion

The smart home resident and administrator can exploit the notification provided by the SIFIS-Home framework related to misbehaviours that occurred in the home. The SIFIS-Home framework will be able to detect physical anomalies by analysing video or audio streaming. The notification will be related to unauthorized persons trying to access the home, attempted performance of forbidden actions or occurring accidents, or when an unusual or forbidden object is brought into the home. The notification will arrive to the smart resident and administrator through a configurable communication channel (e.g., email or SMS), thus making it possible to promptly react to the detected anomaly.

Main actors:

- Smart home resident
- Smart home administrator

Acceptance test:

The smart home resident and administrator must be notified as soon as an unauthorized person has accessed the smart home, or a dangerous situation is detected.

Storyboard (Figure 6):

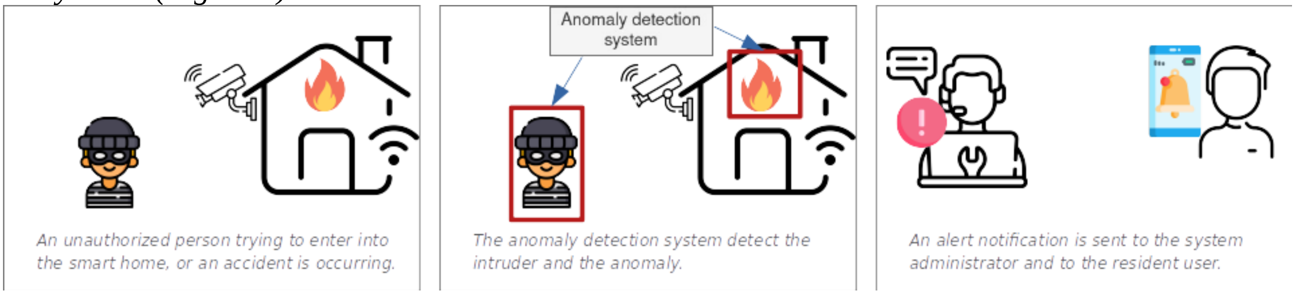

Anomaly detection system
An unauthorized person trying to enter into the smart home, or an accident is occurring.
The anomaly detection system detect the intruder and the anomaly.
An alert notification is sent to the system administrator and to the resident user.

Figure 6. A storyboard of Smart home resident to handle a physical anomaly

4.1.4 SIFIS-US-04: Software anomaly detection in smart home

As a

Smart home administrator

I want to

be notified if some software intrusion is currently taking place

So that

I can take countermeasures to react to the attack.

Discussion

The smart-home administrator can exploit the SIFIS-Home framework's notification related to the software anomalies detected in the home devices or smart home network. The software anomalies will be related to the unauthorized access to a smart device, malware or network attack to compromise nodes or steal sensitive information. The SIFIS-Home framework exploiting a software and network intrusion detection system will notify the smart home administrator through a configurable communication channel (e.g., email or SMS) thus making it possible to promptly react to the attack.

Main actors:

- Smart home administrator

Acceptance test:

- The smart home administrator must be notified as soon as a software intrusion is detected in the smart home system.

Storyboard (Figure 7):

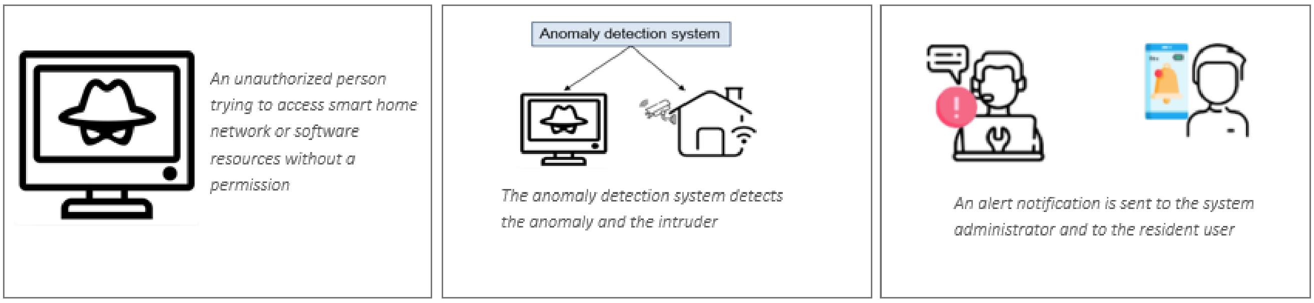

An unauthorized person trying to access smart home network or software resources without a permission
Anomaly detection system
The anomaly detection system detects the anomaly and the intruder
An alert notification is sent to the system administrator and to the resident user

Figure 7. A storyboard of Smart home administrator to notice a software intrusion

4.1.5 SIFIS-US-05: Register/Unregister device in the smart home

As a

Smart home resident/administrator

I want to

register and unregister new devices in the smart home

So that

I can use them in the smart home through the supervision of the SIFIS-Home framework.

Discussion

The smart home resident or administrator user must have the possibility to register and unregister a new device (smart or not so smart) to the smart home system managed by the SIFIS-Home framework. The system will allow the user to register a new device and to specify the configuration settings related to how it must operate. The device will be added to the user profile of the person who registered it to enable them to unregister the device and modify its settings. After the registration, the device will be available to interact through the SIFIS-Home framework and could be managed by the smart home administrator or the resident user. The system will allow having regulated and time-limited registrations, e.g. on daily or weekly basis, for devices that have to be used only for a limited amount of time.

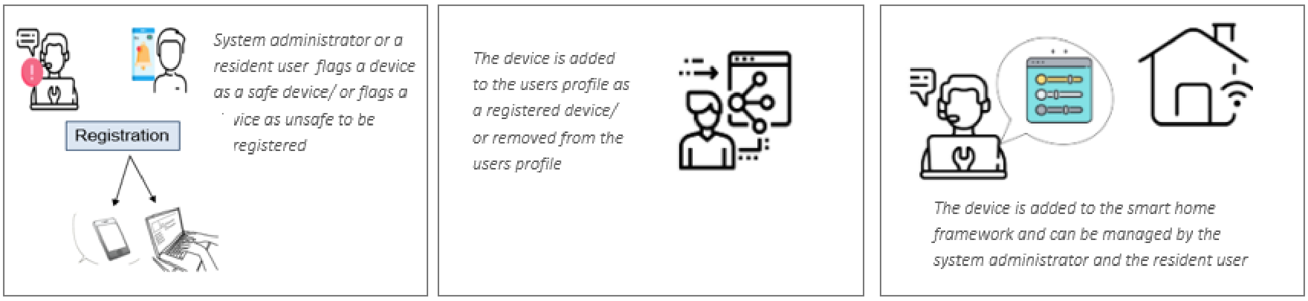
Main actors:

- Smart home resident
- Smart home administrator

Acceptance test:

- The actor must have the possibility to register/unregister a new device in the smart home.
- The device must be added to the user profile of the person who registered it.
- The device must be available to be managed by the resident user and system administrator.

Storyboard (Figure 8):



System administrator or a resident user flags a device as a safe device/ or flags a vice as unsafe to be registered

The device is added to the users profile as a registered device/ or removed from the users profile

The device is added to the smart home framework and can be managed by the system administrator and the resident user

Figure 8. A storyboard of Smart home resident to register/unregister a new device

4.1.6 SIFIS-US-06: Installing third-party application

As a

Smart home administrator/resident

I want to

Install a new third-party application in specific devices

So that

I can use it in the SIFIS-Home ecosystem

Discussion

The smart home administrator or resident user must have the possibility to install new functionalities in a specific device by installing a third-party application. The SIFIS-Home framework will check the smart home policies against the security and safety aspect of the application and its functionalities. If the check is successful, the SIFIS-Home framework allows for the application to be installed. Otherwise, if some policies are violated, the installation procedure will not start.

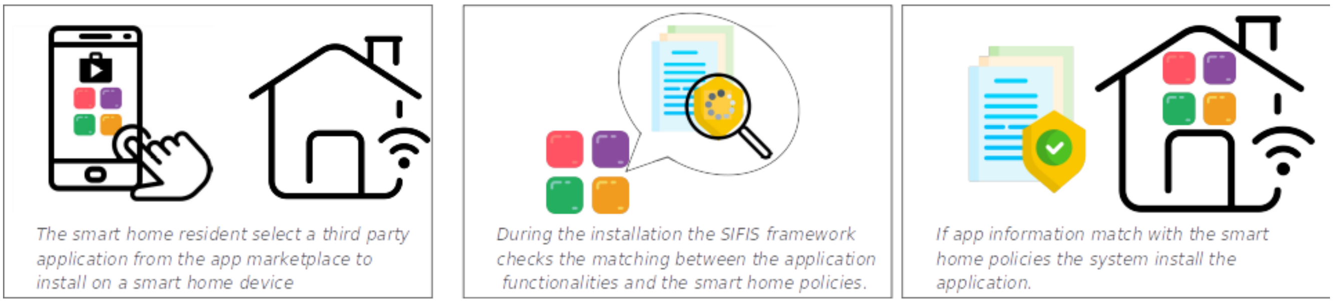
Main actors:

- Smart home resident.
- Smart home administrator.

Acceptance test:

- The SIFIS-Home framework must allow the installation of a third-party application that matches the smart home policies.
- The SIFIS-Home framework must block the installation of a third-party application that does not match the smart home policies.

Storyboard (Figure 9)



The smart home resident select a third party application from the app marketplace to install on a smart home device

During the installation the SIFIS framework checks the matching between the application functionalities and the smart home policies.

If app information match with the smart home policies the system install the application.

Figure 9. A storyboard of Smart home resident to install a new third-party application

4.1.7 SIFIS-US-07: Creation and management of user profiles

As a

Smart home administrator/resident.

I want to

be able to create user profiles of different types and privileges and assign devices and applications to those profiles.

So that

profiles can be managed, and network can be monitored easily.

Discussion

The system administrator or a resident user must have the possibility to create a new user profile that can operate in the smart home. It is possible to provide privileges and assign devices/operations and applications to the new user profile. In addition, the actor can specify their preferences and enforcement conditions.

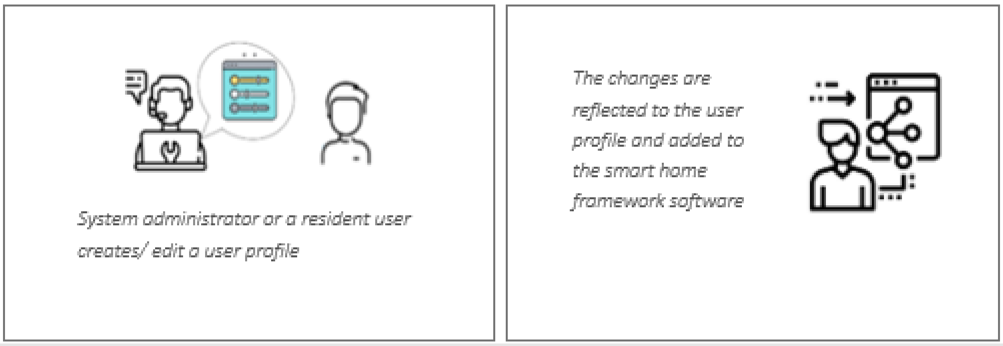
Main actors:

- Smart home resident
- Smart home administrator.

Acceptance test

- The actor must have the possibility to create a new user profile assigning them custom privileges and the device and application allowed.

Storyboard (Figure 10):



System administrator or a resident user creates/ edit a user profile

The changes are reflected to the user profile and added to the smart home framework software

Figure 10. A storyboard of Smart home resident to manage a user profile

4.2 *Use Case Diagram and Narratives*

Decomposing system requirements into fundamental use cases is performed to define the basic structure of the system and the functionalities that should be delivered and validated [Jacobson, 2004]. Figure 11 reports the full Use Case Diagram of the SIFIS-Home system. The human actors interacting with the system reflect the human actors identified in the Context Diagram (described in the previous section) and in the User Stories from which the Use Cases are elicited. The Use Case Diagram highlights the hierarchy of dependencies between the different users. Users that are at lower levels in the hierarchy inherit all the use cases of the users higher in the hierarchy. Detailed description of the use cases, in the form of Use Case Narratives, are reported in the fourteen sub-sections of this Section 4.2. Accordingly, we provide the narratives for each use case, specifying goals, triggers, users and steps of each of the fourteen use cases shown in the use case diagram.

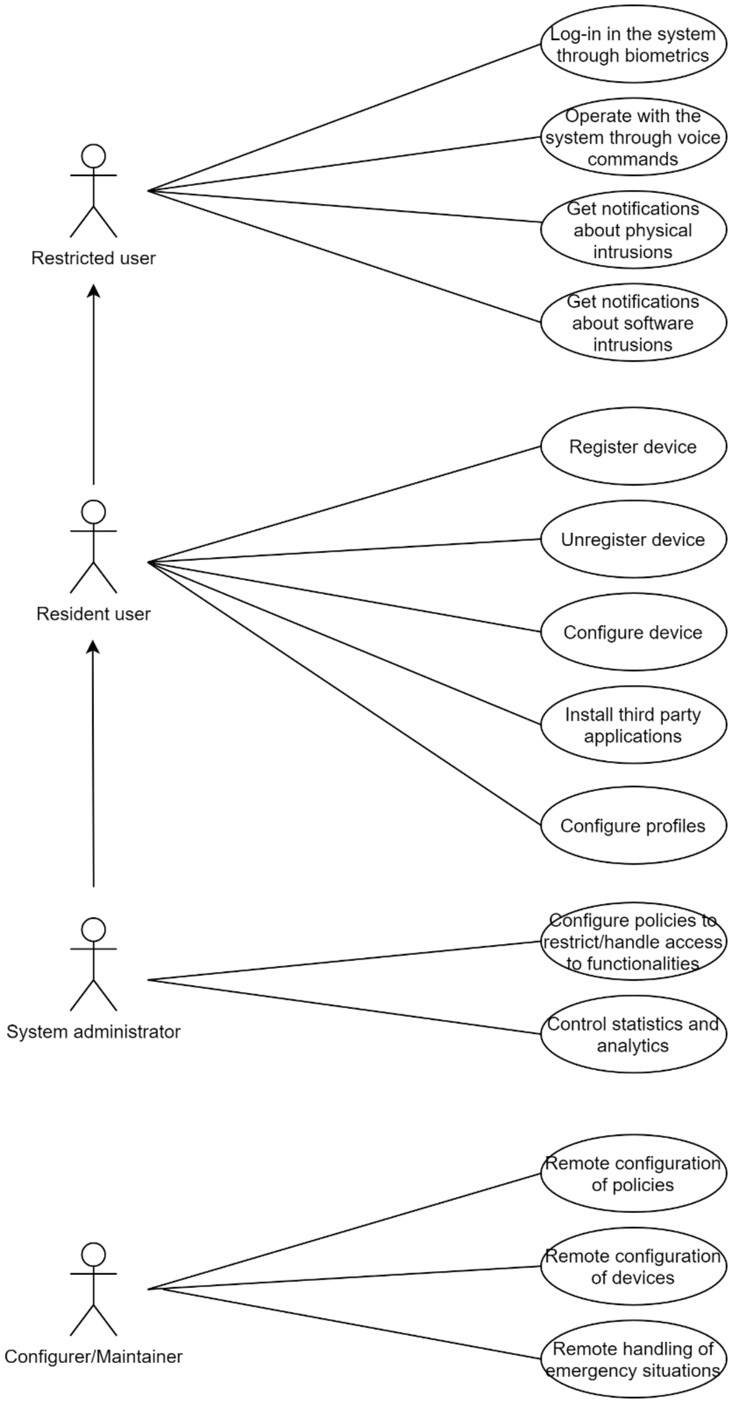

Restricted user
Log-in in the system through biometrics
Operate with the system through voice commands
Get notifications about physical intrusions
Get notifications about software intrusions
Resident user
Register device
Unregister device
Configure device
Install third party applications
Configure profiles
System administrator
Configure policies to restrict/handle access to functionalities
Control statistics and analytics
Configurer/Maintainer
Remote configuration of policies
Remote configuration of devices
Remote handling of emergency situations

Figure 11. The full use case diagram of the SIFIS-Home system

4.2.1 SIFIS-UC-01: Log-in in the system through biometrics

Use Case #	SIFIS-UC-01
Goal in Context	The users want to be identified with biometrics for authentication or to receive dedicated services.
Scope & Level	User Goal
Preconditions	User is registered in the system.
Success End Conditions	The user is recognised and authorised to do specific actions according to the identity.
Failed End Condition	Voice commands are not recognised, and only low privileges operations are allowed.

Primary, Secondary Actors	Restricted User, Administrator
Trigger	-
Description	1. The user interacts (directly or indirectly) with a device reading biometrics (e.g., camera, smart speaker).
	2. The biometrics data is read.
	3. The identity is matched with the known ones.
	4. Specific actions are allowed or functionalities are activated according to policies and profiles.
Extensions	
	4a. The identity is not recognised and a guest profile is applied.
	4b. The identity is not recognised and no residents in the home authorized the access. The person is considered as an intruder.

4.2.2 SIFIS-UC-02: Operate with the system through voice commands

Use Case #	SIFIS-UC-02
Goal in Context	Give voice commands to devices registered in the system.
Scope & Level	User Goal
Preconditions	User is registered in the system.
Success End Conditions	Voice commands are correctly handled by devices of the SIFIS-Home system.
Failed End Condition	Voice commands are not recognised by devices of the SIFIS-Home system and a new input is requested.
Primary, Secondary Actors	Restricted User, Administrator
Trigger	-
Description	1. The user gives a voice command to start the interaction with the system.
	2. The system asks which type of command the user wants to execute.
	3. The user gives the specific voice command.
	4. The system executes the command.
Extensions	1a. The command can also be issued via other input peripherals.
	3a. The user does not provide any command. The interaction fails.
	4a. The system does not recognise the command. The system asks the user to repeat the command. The interaction goes to step 3.
	4b. The command cannot be executed by the device that captured it. It is forwarded to the device able to execute it (if any).

4.2.3 SIFIS-UC-03: Get notifications about physical intrusions

Use Case #	SIFIS-UC-03
Goal in Context	Notify the user of an ongoing physical intrusion.
Scope & Level	Emergency management
Preconditions	Motion sensors and/or cameras are installed in the smart home.
Success End Conditions	The intrusion is detected and the users are notified.
Failed End Condition	-
Primary, Secondary Actors	Restricted User, Maintainer
Trigger	An intruder enters the smart home without authorisation; the

	intrusion is noticed by motion sensors and cameras and the alarm system is activated.
Description	1. The system shows a notification to the user about the intrusion.
Extensions	1a. Cameras start recording the intruders actions and store the identity if the face is recognized. The recording can be analysed by the maintainer.
	1b. Authorities are contacted to give assistance.

4.2.4 SIFIS-UC-04: Get notifications about software intrusions

Use Case #	SIFIS-UC-04
Goal in Context	Notify the user of an ongoing software intrusion (malware).
Scope & Level	Emergency management
Preconditions	An anomalous behaviour can be identified.
Success End Conditions	The intrusion is detected, and the users are notified.
Failed End Condition	-
Primary, Secondary Actors	Restricted User, Maintainer
Trigger	Malware is installed on a smart device and the malicious code or behaviour is identified by the system.
Description	1. The system notifies the user about the installation of malicious code
Extensions	1a. Self-healing algorithm is used to transfer functionalities of isolated device to others (if possible).
	1b. Maintainer or administrator verifies that the malware has not spread to other devices.

4.2.5 SIFIS-UC-05: Register device

Use Case #	SIFIS-UC-05
Goal in Context	Registering a new device in the SIFIS-Home network.
Scope & Level	User Goal
Preconditions	Resident user is logged in the system.
Success End Conditions	A new device is registered in the SIFIS-Home network.
Failed End Condition	No device is registered in the SIFIS-Home network.
Primary, Secondary Actors	Resident User
Trigger	-
Description	1. The user opens the feature “Register new device”
	2. The system prompts the user version of the page with device characteristics to be inserted.
	3. The user inputs the characteristics and the name of the device.
	4. The system shows a recap of the information and asks the user for confirmation.
	5. The user confirms the registration.
	6. The system confirms that the registration is successful.
Extensions	3a. The user quits ahead of time. The interaction ends with failure.
	3b. The user selects a temporary registration for the device.
	5a. The user does not confirm the registration. The interaction ends with failure.
	6a. The registration is not successful. The system prompts the user with an error.

4.2.6 SIFIS-UC-06: Unregister device

Use Case #	SIFIS-UC-06
Goal in Context	Removing a device from the list of registered ones in the SIFIS-Home network.
Scope & Level	User Goal
Preconditions	Resident user is logged in the system.
Success End Conditions	The selected device is no-longer present in the list of registered devices of the SIFIS-Home network.
Failed End Condition	No changes in the list of registered devices.
Primary, Secondary Actors	Resident User
Trigger	-
Description	1. The user opens the feature “Unregister device”
	2. The system prompts with the list of registered devices to the SIFIS-Home network.
	3. The user selects the device to unregister.
	4. The system shows the information of the device to unregister.
	5. The user confirms the decision of unregistering the device.
	6. The system prompts the user that the operation is successful.
Extensions	3a. The user quits ahead of time. The interaction ends with failure.
	5a. The user aborts the decision of unregistering the device. The interaction ends with a failure.
	6a. It is not possible to unregister the device. The system prompts the user with an error.

4.2.7 SIFIS-UC-07: Configure device

Use Case #	SIFIS-UC-07
Goal in Context	Changing the settings for a device in the list of registered devices in the SIFIS-Home network.
Scope & Level	User Goal
Preconditions	Resident user is logged in the system.
Success End Conditions	The desired modifications in the settings are successfully applied for the selected device.
Failed End Condition	No changes in the settings.
Primary, Secondary Actors	Resident User
Trigger	-
Description	1. The user opens the feature “Device settings”
	2. The system prompts with the list of registered devices to the SIFIS-Home network.
	3. The user selects the device to configure.
	4. The system shows the configuration options for the user.
	5. The user selects the desired configuration options and clicks “save”.
	6. The system asks for confirmation to save the changes.
	7. The user confirms the changes.
	8. The system prompts the user that the operation is successful.
Extensions	3a. The user quits. The use case ends with failure.
	5a. The user quits. The use case ends with failure.

	7a. The user does not confirm the changes. The interaction goes back to step 4.
	8a. The system is not able to propagate the desired modifications to the configuration. The user is prompted with an error message.
	8b. An external event alters the context against the current configuration. The devices act autonomously to change the context according to configuration.

4.2.8 SIFIS-UC-08: Installing third-party applications

Use Case #	SIFIS-UC-08
Goal in Context	Install new functionalities in specific devices by installing third-party applications.
Scope & Level	User Goal
Preconditions	Resident user is logged in the system.
Success End Conditions	The application is integrated in the SIFIS-Home system.
Failed End Condition	The application violates the smart home policies and is not installed.
Primary, Secondary Actors	Resident User, Maintainer
Trigger	-
Description	1. The user opens the app marketplace and selects a new app.
	2. The user is notified about security and safety aspects of the app.
	3. The user confirms the intention to install the applications.
	4. App information is matched with smart home policies. The system installs the application and notifies it to the user.
Extension	2a. The user does not want to install the application: the interaction ends with failure.
	4a. The app is not compatible with the smart home policies. The interaction ends with failure.

4.2.9 SIFIS-UC-09: Configure policies to restrict/handle access to functionalities

Use Case #	SIFIS-UC-09
Goal in Context	Define policies and access rights to smart home functionalities to the various users and installed applications.
Scope & Level	User Goal
Preconditions	- Administrator is logged in the SIFIS-Home framework - Administrator has a smart device with GUI
Success End Conditions	The administrator successfully configures enforceable policies.
Failed End Condition	The administrator is not able to configure enforceable policies.
Primary, Secondary Actors	Administrator, Maintainer
Trigger	-
Description	1. The administrator opens the configuration panel on a smart device with GUI or remotely from a PC or smartphone and selects the feature to handle policies.
	2. The system asks the administrator to select the user/application to configure.
	3. The administrator selects a specific user or user group, or installed applications.
	4. The system shows the list of action/resources that can be allowed or forbidden.

	5. The administrator selects the list of allowed/forbidden action/resources for the user/application.
	6. The system saves the change. The policy enforcement starts upon saving. User is notified.
Extensions	3a. User leaves. Interaction ends with failure.
	5a. User leaves. Interaction ends with failure.
	6a. The change cannot be saved. Interaction ends with failure.

4.2.10 SIFIS-UC-10: Configure user settings

Use Case #	SIFIS-UC-10
Goal in Context	Define different usage profiles based on involved users, time of the day and security preferences.
Scope & Level	User Goal
Preconditions	- User is logged in the SIFIS-Home framework - User interacts with a smart device accepting voice commands or has a GUI.
Success End Conditions	The framework is able to define profiles to provide different working properties and conditions.
Failed End Condition	Profiles are not configurable or do not activate when needed.
Primary, Secondary Actors	Resident User
Trigger	-
Description	1. The resident opens the configuration panel on a smart device through its GUI or remotely from a PC or smartphone, or gives a voice command, and selects the feature to configure profiles.
	2. The system shows the menu for configuration of profiles.
	3. The resident specifies their preferences and enforcement conditions.
	4. The system shows the summary of preferences and asks the user for confirmation.
	5. The user confirms.
	6. The preference is saved and enforced according to specified conditions. The user is notified.
Extensions	3a. User leaves. Use case ends with failure.
	5a. User leaves or does not confirm. Use case ends with failure.
	6a. It is impossible to save the configuration. Use case ends with failure.
	7. An external event alters the context against the current configuration. The devices act autonomously to change the context according to configuration.

4.2.11 SIFIS-UC-11: Control Statistics and Analytics

Use Case #	SIFIS-UC-11
Goal in Context	Visualize analysis about the system activities and status.
Scope & Level	User Goal
Preconditions	- Administrator is logged in the SIFIS-Home network - Administrator has a smart device with GUI
Success End Conditions	The framework provides graphic statistics and analytics about the system.
Failed End Condition	The required information is not shown to the administrator.

Primary, Secondary Actors	Administrator
Trigger	-
Description	1. The administrator opens the feature “system analytics”.
	2. The system opens the analytics menu with menu voices about device, user and profile usage.
	3. The administrator selects the device, user or profile for which (s)he wants to see usage analytics.
	4. The system shows a GUI with the required analytics.
Extensions	3a. User leaves. The interaction ends with failure.
	4a. The system is not able to provide the required analytics. The interaction ends with failure.

4.2.12 SIFIS-UC-12: Remote Configuration of devices

Use Case #	SIFIS-UC-12
Goal in Context	Configure specific device functionalities remotely.
Scope & Level	User Goal
Preconditions	- Configurer is logged in the System - Configurer is enabled for the configuration of the smart home by the administrator.
Success End Conditions	The framework provides a GUI on which the configurer successfully sets up device functionalities.
Failed End Condition	Device configuration is not possible.
Primary, Secondary Actors	Configurer
Trigger	-
Description	1. The configurer opens the control panel for configuration.
	2. The system shows the homes that the configurer is allowed to manage.
	3. The configurer selects the smart home where the device is located.
	4. The system shows the list of devices in the smart home.
	5. The configurer selects the device to configure.
	6. The system shows the configuration options for the device.
	7. The configurer selects the desired configuration options and saves the changes.
	8. The system asks for confirmation to save the changes.
	9. The user confirms the changes.
	10. The system prompts the user that the operation is successful.
Extensions	3a. The user leaves. Interaction ends with failure.
	4a. It is not possible to retrieve the list of devices. The interaction ends with failure.
	5a. The user leaves. Interaction ends with failure.
	7a. The user leaves. Interaction ends with failure.
	9a. The user leaves. Interaction ends with failure.
	10a. It is not possible to apply the configuration changes. Interaction ends with failure.

4.2.13 SIFIS-UC-13: Remote Configuration of policies

Use Case #	SIFIS-UC-13
Goal in Context	Remotely define policies and access rights to smart home functionalities to the various users and installed applications.
Scope & Level	User goal
Preconditions	The smart home has Internet connectivity. The administrator allows access to the configurator. The configurer is logged in the system.
Success End Conditions	The framework provides a GUI through which the administrator successfully configures device functionalities.
Failed End Condition	Device configuration is not possible.
Primary, Secondary Actors	Configurer, Administrator
Trigger	User opening the policy configuration panel.
Description	1. The configurer opens the control panel for configuration of policies.
	2. The system shows the homes that the configurer is allowed to manage.
	3. The Configurer selects the smart home where the policy must be changed.
	4. The System shows the list of policies configured in the smart home.
	5. The Configurer selects the policy to configure.
	6. The system shows the configuration options for the policy.
	7. The configurer selects the desired configuration options and clicks “save”.
	8. The system asks for confirmations to save the changes.
	9. The user confirms the changes.
	10. The system prompts the configurer that the operation is successful and notifies the administrator about the new/updated policy.
	11. The smart home administrator accepts the new/updated policy.
Extensions	3a. The user leaves. Interaction ends with failure.
	4a. It is not possible to retrieve the list of devices. The interaction ends with failure.
	5a. The user leaves. Interaction ends with failure.
	7a. The user leaves. Interaction ends with failure.
	9a. The user leaves. Interaction ends with failure.
	10a. It is not possible to apply the policy changes. Interaction ends with failure.
	11a. The administrator does not accept the policy change. The interaction ends with failure.

4.2.14 SIFIS-UC-14: Remote handling of emergency situations

Use Case #	SIFIS-UC-14
Goal in Context	Configurer wants to access to the smart home functionality remotely in order to quickly react to an emergency.
Scope & Level	User goal
Preconditions	- Configurer is registered in the SIFIS-Home framework - Configurer is allowed by the Administrator for the management of

	emergency situations in the smart home.
Success End Conditions	The framework allows the configurer to log in remotely to remotely manage emergency situations.
Failed End Condition	The configurer cannot remotely access the smart home environment and react to the emergency situation.
Primary, Secondary Actors	Configurer
Trigger	A physical or software intrusion in the SIFIS-Home network is detected.
Description	1. The system notifies the Configurer about the intrusion.
	2. The configurer selects the action to take against the intrusion.
Extensions	1a. Authorities are contacted to give assistance.
	1b. Cameras record the intrusion (in case of physical intrusion).

4.3 *Catalogue of use cases*

In Table 4, we report the mapping between the use cases and the user stories. Each user story is related to at least one use case.

	SIFIS-US-01	SIFIS-US-02	SIFIS-US-03	SIFIS-US-04	SIFIS-US-05	SIFIS-US-06	SIFIS-US-07
SIFIS-UC-01	***X***						
SIFIS-UC-02	***X***						
SIFIS-UC-03			***X***				
SIFIS-UC-04				***X***			
SIFIS-UC-05					***X***		
SIFIS-UC-06					***X***		
SIFIS-UC-07		***X***					
SIFIS-UC-08						***X***	
SIFIS-UC-09		***X***					
SIFIS-UC-10							***X***
SIFIS-UC-11		***X***					
SIFIS-UC-12		***X***					
SIFIS-UC-13		***X***					
SIFIS-UC-14			***X***				

Table 4. Mapping between use cases and user stories

5 Requirements

In Table 5, we report the Functional Requirements that have been elicited for the SIFIS-Home system. For each requirement, we report a brief description, the use case(s) to which it relates to (or none, if it is a general requirement of the system), the type and priority of the requirement, a unique ID for the requirements document, the pointers to corresponding non-functional requirements and their types.

We prioritize the requirements according to the following scheme:

- ***Critical***: a requirement that must be fulfilled for the execution of the essential system functionalities.
- ***Standard***: a requirement that should be fulfilled but whose non-fulfilment does not impair the execution of the essential system functionalities.
- ***Optional***: a requirement that may be fulfilled but whose non-fulfilment does not impair the execution of the system functionalities.

The requirements presented in the following are the finalized list of elicited requirements after receiving feedbacks from D3.1 and D4.1 related to technical aspects of the SIFIS-Home framework and architecture. We will report also a discussion on how the comments have been addressed.

5.1 *Functional Requirements*

In the following, we report the list of functional requirements identified for the SIFIS-Home architecture. All requirements identified are derived from the defined use cases. Table 5 also reports the mapping with the non-functional requirements (NFR) defined in the following section and the prioritisation level.

In Table 5, we report the requirements after the refinement that took into account the comments on the requirements provided by deliverables D3.1 and D4.1 We report in Table 6 the original requirements table from deliverable D1.1, with a summary of such comments.

All the requirements were refined or amended according to the comments from deliverables D3.1 and D4.1. Major modifications of the requirements involved the removal of the original F-06, which was overlapping with F-01 and F-05, and the split of F-12 into two separate requirements. The requirements suggested from deliverable D3.1 and D4.1 were added to the table of requirements. Finally, the requirements were consistently re-numbered.

ID	Req. description	UC	Priority	NFR-Req. ID	NFR- Req. Type
F-01	The SIFIS-Home framework shall provide means of identifying the resident users and administrators inside the smart home through biometrics.	UC1	C	PE-03 US-09 DE-01	Performance Usability Dependability
F-02	The SIFIS-Home system shall provide means of authentication to resident users, administrators and guest users inside the smart home.	UC1	C	PE-01	Performance
F-03	The SIFIS-Home system shall match read biometrics against a database of stored ones, in order to assess authentication.	UC1	S	PE-01 PE-04	Performance Performance
F-04	The system shall make different features available and accessible to different users, based on their authenticated identity	UC1	S	PE-05	Performance
F-05	The system shall activate a guest profile when the identity of the biometrics is not recognised.	UC1	S	PE-05	Performance
F-06	The SIFIS-Home system shall provide Automatic Speech Recognition (ASR) to provide resident users and	UC2	C	PE-02 PE-06	Performance Performance

	administrators the facility to control their home appliances through their speech.			DE-02 DE-03	Dependability Dependability
F-07	The SIFIS-Home system shall have means to receive and interpret the voice commands provided by the user, and it shall be able to interpret those commands belonging to a predefined command set	UC2	C	PE-07	Performance
F-08	The SIFIS-Home system shall be able to execute a predefined set of actions in response to a predefined set of recognizable voice commands	UC2	C	PE-08	Performance
F-09	The SIFIS-Home system shall signal the presence of an intruder when the identity is not recognised and no residents are at home.	UC3	C	US-10	Usability
F-10	The SIFIS-Home system, following the detection of an intruder, shall track the intruder and attempt again to identify him/her	UC3, UC14	C	DE-04	Dependability
F-11	The SIFIS-Home system shall store the identity of the intruder if the face is recognized. If the face is not recognized, the video and audio recordings must be stored from the system as well	UC3, UC14	C	DE-05	Dependability
F-12	The SIFIS-Home system, following the detection of an intruder, shall track the intruder and attempt again to identify him/her.	UC3, UC14	C	DE-05	Dependability
F-13	The SIFIS-Home system may grant the access to recording to the maintainer.	UC3, UC14	S	PE-09 US-10	Performance Usability
F-14	The SIFIS-Home system may allow administrators and resident users to contact police to receive assistance in case of intrusions	UC3, UC14	O	PE-10	Performance
F-15	The SIFIS-Home system shall provide means of identifying anomalous situations and behaviours inside the smart home	UC3, UC14	C	PE-10	Performance
F-16	The SIFIS-Home system shall provide means of recognition of allowed users in unusual locations or performing dangerous actions, and signal them to resident users and administrators.	UC3, UC14	S	PE-10	Performance
F-17	The SIFIS-Home system shall provide means of recognition of prohibited objects inside the smart home and signal resident users and administrators.	UC3, UC14	S	PE-10	Performance
F-18	The SIFIS-Home system shall provide means of recognition of allowed objects inside the smart home in unusual positions, and signal resident users and administrators.	UC3, UC14	O	PE-10	Performance
F-19	The SIFIS-Home system shall detect, identify and disconnect infected devices.	UC4	C	PE-11 US-11 DE-06	Performance Usability Dependability
F-20	The SIFIS-Home system shall notify resident users and administrators when malware is detected.	UC4	C	PE-12 US-11	Performance Usability
F-21	The SIFIS-Home system shall be able to execute self-healing algorithms to transfer functionalities of devices that have been disconnected for security reasons to the others.	UC4	C	PE-13 DE-06	Performance Dependability
F-22	The SIFIS-Home system should allow means of verifying that the malware has not spread to other devices.	UC4	S		
F-23	The SIFIS-Home system shall allow the resident user to register more components to the system.	UC5	C	PE-14 US-12 DE-07	Performance Usability Dependability

F-24	The SIFIS-Home system shall allow the resident users and administrators to visualize a list of the registered devices, along with their characteristics.	UC5, UC6, UC7, UC12	C	PE-15	Performance
F-25	The SIFIS-Home system shall allow the administrators and device owners to unregister from the system a registered component.	UC6, UC12	C	PE-16 DE-08	Performance Dependability
F-26	The SIFIS-Home systems shall expose a section where the device owners and administrators can configure the devices.	UC7	C	PE-17, PE-18 US-13 US-14 DE-09 DE-10	Performance Performance Usability Usability Dependability Dependability
F-27	The SIFIS-Home system shall prompt the administrator when unsolicited configuration changes are propagated to the devices.	UC7, UC12	S	PE-18	Performance
F-28	The SIFIS-Home system must provide a marketplace function for the download of third-party applications on smart devices.	UC8	C	PE-19 US-15 DE-11	Performance Usability Dependability
F-29	The SIFIS-Home system shall retrieve and provide information about the safety and security aspects of an application to the user.	UC8	C		
F-30	The SIFIS-Home system must provide a feature to show the administrators a list of currently active policies.	UC9, UC13	S	PE-22	Performance
F-31	The SIFIS-Home system must provide a feature to show the administrators a list of currently active policies	UC9, UC13	C	DE-12	Dependability
F-32	The SIFIS-Home system must allow the administrator to configure policies for (groups of) users.	UC9, UC13	S	PE-20 US-16	Performance Usability
F-33	The SIFIS-Home system must allow the administrator to configure policies for (groups of) devices.	UC9, UC13	S	PE-21 US-17 DE-12	Performance Usability Dependability
F-34	The SIFIS-Home system must allow the administrator to view the policies related to features and/or resources either permitting or denying access or usage to (groups of) users.	UC9, UC13	S	DE-12	Dependability
F-35	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of devices.	UC9, UC13	S		
F-36	The SIFIS-Home system must provide the user with a feature to list all the currently available profiles.	UC10	S		
F-37	The SIFIS-Home system must allow the user to configure his/her profiles.	UC10	S	PE-23 US-18 DE-13	Performance Usability Dependability
F-38	The SIFIS-Home system may allow the user to switch his/her current profile.	UC10	O	PE-24 US-19 DE-14	Performance Usability Dependability
F-39	The SIFIS-Home system should show the user a summary of the preferences associated to its current profile.	UC10	O		
F-40	The SIFIS-Home system should show notifications to the user when the current profile is changed.	UC10	O		
F-41	The SIFIS-Home system should offer aggregate analytics and statistics about the usage and behaviour of devices to the administrator.	UC11	S	PE-25 US-20 DE-15	Performance Usability Dependability
F-42	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of profiles to the administrator.	UC11	S	PE-26	Performance
F-43	The SIFIS-Home system must offer remote authenticated and secure log-in features to configurer/maintainers of user profiles.	UC12, UC13	S	PE-27 DE-16	Performance Dependability

F-44	The SIFIS-Home system shall offer to the maintainers a panel with the remote homes he/she can manage.	UC13	S		
F-45	The SIFIS-Home system must offer the maintainer an interface with the possibility to call the authorities or alert the administrator and residents, in case of intrusions.	UC14	S		
F-46	The SIFIS-Home system shall allow the residents to store personal content (video, audio, text).	UC10	C		
F-47	The SIFIS-Home system must be able to map a policy defined by the administrator into one or more device-level policies.	all	C	TE-01 AV-01 DE-20	Technical Availability Dependability
F-48	The SIFIS-Home should be able to map the device-level policies with the capabilities of the involved devices.	all	C	PE-25 US-20 DE-15	Technical Availability Dependability
F-49	The SIFIS-Home must be able to apply the active device-level policies to the actual devices.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
F-50	The SIFIS-Home must be able to apply the active device-level policies when needed.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
F-51	The SIFIS-Home should notify when a device-level policy cannot be mapped onto any device.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
F-52	The SIFIS-Home should be able to identify redundant or conflicting policies.	all	S	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
F-53	The description of the policies must be available to administrators, maintainers and tenants of the SIFIS-Home system.	all	C	TE-02	Technical
F-54	Administrators and configurers shall be able to create, configure and delete security groups.	UC5, UC6, UC7, UC12	C		

F-55	Administrators and configurers shall be able to register security groups and thus make them dynamically discoverable	UC5, UC6, UC7, UC12	C		
F-56	There must be a means for Administrators and devices to discover security groups, including their properties, how to join them, as well as their associations with application groups and their resources.	UC5, UC6, UC7, UC12	C		
F-57	There must be a means for devices to join/leave a security group and retrieve/provide updated key material to communicate in the group	UC5, UC6, UC7, UC12	C		

Table 5. The list of final functional requirements for the SIFIS-Home system

Table 6 reports the list of original Functional Requirements elicited for the SIFIS-Home system. Column “Feedback” summarizes the input provided by deliverables D3.1 and D4.1, that was taken into account to revise the requirements in the final requirements table of the present deliverable. The feedback for each requirement is categorized as “OK”, “Refine”, or “Amend”. The requirements to add according to deliverable D3.1 and D4.1 are reported at the end of the table.

ID	Req. description	UC	Priority	NFR-Req. ID	NFR-eq. R Type	Feedback
F-01	The SIFIS-Home framework shall provide means of identifying the users inside the smart home through biometrics.	UC1	C	PE-03 US-09 DE-01	Performance Usability Dependability	R
F-02	The SIFIS-Home system shall provide means of authentication to the resident users and administrators inside the smart home.	UC1	S	PE-01	Performance	R
F-03	The SIFIS-Home system shall match read biometrics with a database of stored ones.	UC1	S	PE-01 PE-04	Performance Performance	O
F-04	The system shall activate features based on the user identity.	UC1	S	PE-05	Performance	O
F-05	The system shall activate a guest profile when the identity of the biometrics is not recognised.	UC1	S	PE-05	Performance	R
F-06	The SIFIS-Home system shall provide means of recognition of allowed users in the smart home.	UC1, UC3	C	PE-02	Performance	R
F-07	The SIFIS-Home system shall provide Automatic Speech Recognition (ASR) to provide the residents the facility to control their home appliances through their speech.	UC2	C	PE-02 PE-06 DE-02 DE-03	Performance Performance Dependability Dependability	R
F-08	The SIFIS-Home system shall receive and interpret the voice commands provided by the user.	UC2	C	PE-07	Performance	R
F-09	The SIFIS-Home system shall be able to execute all the recognisable voice commands.	UC2	C	PE-08	Performance	R
F-10	The SIFIS-Home system shall signal the presence of an intruder when the identity is not recognised and no residents are at home.	UC3	C	US-10	Usability	O
F-11	The SIFIS-Home system shall record intruder actions through cameras.	UC3, UC14	S	DE-04	Dependability	O
F-12	The SIFIS-Home system shall store the identity of the intruder if the face is recognised.	UC3, UC14	O	DE-05	Dependability	R/A
F-13	The SIFIS-Home system may grant the access to recording to the maintainer.	UC3, UC14	S	PE-09 US-10	Performance Usability	R
F-14	The SIFIS-Home system may allow to contact police to receive assistance in case of intrusions.	UC3, UC14	O	PE-10	Performance	R

F-15	The SIFIS-Home system shall provide means of identifying anomaly behaviours inside the smart home.	UC3, UC14	C	PE-10	Performance	O
F-16	The SIFIS-Home system shall provide means of recognition of allowed users in unusual locations or performing dangerous actions.	UC3, UC14	S	PE-10	Performance	R
F-17	The SIFIS-Home system shall provide means of recognition of forbidden objects inside the smart home.	UC3, UC14	S	PE-10	Performance	R
F-18	The SIFIS-Home system shall provide means of recognition of allowed objects in unusual positions.	UC3, UC14	O	PE-10	Performance	R
F-19	The SIFIS-Home system shall identify and isolate infected devices.	UC4	C	PE-11 US-11 DE-06	Performance Usability Dependability	R
F-20	The SIFIS-Home system shall notify the user when malware is detected.	UC4	C	PE-12 US-11	Performance Usability	R
F-21	The SIFIS-Home system may execute self-healing algorithms to transfer functionalities of isolated devices to the others.	UC4	C	PE-13 DE-06	Performance Dependability	R
F-22	The SIFIS-Home system may allow means of verifying that the malware has not spread to other devices.	UC4	S			O
F-23	The SIFIS-Home system shall allow the resident user to register a new device.	UC5	C	PE-14 US-12 DE-07	Performance Usability Dependability	A
F-24	The SIFIS-Home system shall provide a list of the registered devices to the user along with their characteristics.	UC5, UC6, UC7, UC12	C	PE-15	Performance	R
F-25	The SIFIS-Home system shall allow the user to unregister a registered device.	UC6, UC12	C	PE-16 DE-08	Performance Dependability	A/R
F-26	The SIFIS-Home systems shall expose a section where the resident users and administrators can configure the devices.	UC7	C	PE-17, PE-18 US-13 US-14 DE-09 DE-10	Performance Performance Usability Usability Dependability Dependability	A
F-27	The SIFIS-Home system shall prompt the user when unsolicited configuration changes are propagated to the devices.	UC7, UC12	S	PE-18	Performance	A
F-28	The SIFIS-Home system must provide a marketplace function for the download of third-party applications on smart devices.	UC8	C	PE-19 US-15 DE-11	Performance Usability Dependability	R
F-29	The SIFIS-Home system shall provide information about the safety and security aspects of an application to the user.	UC8	C			O
F-30	The SIFIS-Home system must provide a feature to show the administrator a list of currently active policies.	UC9, UC13	S	PE-22	Performance	O
F-31	The SIFIS-Home system must allow the administrator to configure the policies to restrict/enable access to functionalities.	UC9, UC13	C	DE-12	Dependability	R
F-32	The SIFIS-Home system must allow the administrator to configure policies for groups of users.	UC9, UC13	S	PE-20 US-16	Performance Usability	R
F-33	The SIFIS-Home system must allow the administrator to configure policies for group of devices.	UC9, UC13	S	PE-21 US-17 DE-12	Performance Usability Dependability	R
F-34	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of users.	UC9, UC13	S	DE-12	Dependability	R
F-35	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or	UC9, UC13	S			R

	forbidden for all groups of devices.					
F-36	The SIFIS-Home system must provide the user with a feature to list all the currently available profiles.	UC10	S			R
F-37	The SIFIS-Home system must allow the user to configure its profiles.	UC10	S	PE-23 US-18 DE-13	Performance Usability Dependability	R
F-38	The SIFIS-Home system must allow the user to switch his/her current profile.	UC10	O	PE-24 US-19 DE-14	Performance Usability Dependability	R
F-39	The SIFIS-Home system should show the user a summary of the preferences associated to its current profile.	UC10	O			R
F-40	The SIFIS-Home system should show notifications to the user when the current profile is changed.	UC10	O			R
F-41	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of devices to the administrator.	UC11	S	PE-25 US-20 DE-15	Performance Usability Dependability	O
F-42	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of profiles to the administrator.	UC11	S	PE-26	Performance	R
F-43	The SIFIS-Home system must offer remote log-in features to configurer/maintainers user profiles.	UC12, UC13	S	PE-27 DE-16	Performance Dependability	R
F-44	The SIFIS-Home system shall offer a panel with the remote houses that can be managed by a maintainer.	UC13	S			R
F-45	The SIFIS-Home system must offer the maintainer a panel to react in case of intrusions.	UC14	S			O
F-46	The SIFIS-Home system shall store personal resident information (video, audio, text).	UC10	C			O
WP3-F-01	Administrators and configurers shall be able to create, configure and delete security groups.	UC5, UC6, UC7, UC12	C	WP3-PE-01, WP3-PE-02	Performance, Performance	
WP3-F-02	Administrators and configurers shall be able to register security groups and thus make them dynamically discoverable	UC5, UC6, UC7, UC12	C	WP3-PE-01, WP3-PE-02	Performance, Performance	
WP3-F-03	There must be a means for Administrators and devices to discover security groups, including their properties, how to join them, as well as their associations with application groups and their resources.	UC5, UC6, UC7, UC12	C	WP3-PE-01, WP3-PE-02	Performance, Performance	
WP3-F-04	There must be a means for devices to join/leave a security group and retrieve/provide updated key material to communicate in the group	UC5, UC6, UC7, UC12	C	WP3-PE-01, WP3-PE-02	Performance, Performance	

WP4-F-01	The system should support multiple languages.	UC-02	S	PE-07 DE-03	Performance Dependability	
WP4-F-02	The SIFIS-Home system must be able to map a policy defined by the administrator into one or more device-level policies.	all	C	TE-01 AV-01 DE-20	Technical Availability Dependability	
WP4-F-03	The SIFIS-Home should be able to map the device-level policies with the capabilities of the involved devices.	all	C	PE-25 US-20 DE-15	Technical Availability Dependability	
WP4-F-04	The SIFIS-Home must be able to apply the active device-level policies to the actual devices.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability	
WP4-F-05	The SIFIS-Home must be able to apply the active device-level policies when needed.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability	
WP4-F-06	The SIFIS-Home should notify when a device-level policy cannot be mapped onto any device.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability	
WP4-F-07	The SIFIS-Home should be able to identify redundant or conflicting policies.	all	S	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability	
WP4-F-08	The description of the policies must be available.	all	C	TE-02	Technical	

Table 6. Comments to the initial list of functional requirements for the SIFIS-Home framework

A set of Functional (and non-functional as well, as it will be shown later), reported comments related to the definition of minimum functionalities of a working instance of the SIFIS-Home framework and architecture. We report this definition in the following:

Minimum functionality: The minimum functionality that must be ensured by an active instance of the SIFIS-Home framework must respect the following requirements:

- Having at least 50% of the active Smart Devices as not compromised (i.e. not misbehaving) and able to communicate with each other;
- Keeping a valid and not compromised DHT-based distributed database for information storage

and retrieval;

- Having the SIFIS-Home framework running on each non-compromised smart device;
- Intrusion detection and policy enforcement services are up and running;

We derive that the SIFIS-Home framework must be able to work also when not connected to the Internet and without the direct interaction of users. NSSDs are not considered as necessary for the minimum functionalities of the SIFIS-Home architecture.

5.2 *Non-Functional Requirements*

In Table 7, we report the list of non-functional requirements which have been extracted from the above list of functional requirements and after the refinement that took into account the comments on the requirements provided by deliverables D3.1 and D4.1. This set of requirements will pose the basis to define both the SIFIS-Home architecture and SIFIS-Home software framework. Fulfilling these requirements is necessary to ensure that the functional requirements are also fulfilled. The non-functional requirements are categorised as pertaining to Performance (PE), Reliability (RE), Availability (AV), Usability (US), Dependability (DE), and Technical (TE). Non-functional Security requirements are collected in the next section.

All requirements were refined or amended according to the comments from deliverables D3.1 and D4.1. Major modifications of the requirements involved the removal of the original PE-03, which was the same as PE-02, the removal of the original US-02 and replaced with the requirement US-20, and the addition of two non-functional requirements PE-27 and PE-28. The requirements suggested from deliverable D4.1 were added to the table of requirements and a glossary table has been defined. Finally, the requirements were consistently re-numbered.

Req. ID	Req. description	FR	Priority	Feedback
PE-01	The user authentication shall happen in less than 2s.	F-02 F-03	Critical	
PE-02	The user recognition (identification/ biometric-based) shall happen in less than 5s.	F-06	Critical	Refined
PE-03	Biometric-based authentication should be performed in less than 5 seconds.	F-03	Standard	
PE-04	Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.	F-04 F-05	Standard	"Activation of features" defined in a glossary table
PE-05	Recognition of the start of an interaction through voice command should be performed in less than 2 seconds.	F-06	Standard	
PE-06	The interpretation of the voice commands provided by the user should be performed in less than 2 seconds.	F-07	Standard	
PE-07	A command should be invoked within 5 seconds from the event that triggered its execution	F-08	Standard	Refined and a separate non-functional requirement has been added: "In case of an incomplete or unsuccessful command execution, an error response should be sent within 5 seconds"
PE-08	The maintainer must be able to access and watch a recording in less than one minute.	F-13	Standard	

PE-09	If requested to, the SIFIS-Home system shall contact law enforcement or private surveillance services to receive assistance in less than 30 seconds.	F-14	Optional	
PE-10	An abnormal (suspicious) behavior caused by a malware shall be identified and notified within 60 seconds	F-19	Optional	
PE-11	The user should be informed of the presence of a malware no later than 5 seconds after the malware is recognized.	F-20	Standard	Refined
PE-12	Self-healing algorithms should be started in less than 60 seconds if available when malware is recognized.	F-21	Critical	
PE-13	The registration of a new device should be completed in less than 30 seconds.	F-23	Standard	
PE-14	The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.	F-24	Standard	
PE-15	The de-registration of a device should be completed in less than 30 seconds.	F-25	Standard	
PE-16	The correct configuration changes should be propagated successfully in less than 30 seconds.	F-26	Critical	1- Refined. 2- Definition of "configuration" and "propagated successfully" have been added to the glossary table. 3- A separate non-functional requirement has been added: "In case of an incomplete or unsuccessful configuration change, an error message should be returned within 5 seconds"
PE-17	The current configuration of a device should be retrieved in less than 10 seconds.	F-26	Standard	
PE-18	The marketplace should be accessible in less than 60 seconds.	F-28	Standard	Refined
PE-19	The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.	F-32	Critical	1- Refined 2- Definitions of "policy" and "user profile" have been added to the glossary table.
PE-20	The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.	F-33	Critical	Refined
PE-21	The list of policies should be retrieved in less than 30 seconds.	F-30	Standard	
PE-22	The configuration of profiles should be applied and enforced in less than 60 seconds.	F-37	Critical	Refined
PE-23	The change of current profile should be performed in less than 60 seconds.	F-38	Critical	Refined to consider "usage modes" instead of "profiles"
PE-24	The statistics about usage and behaviour of devices should be presented to the administrator in less than 30 seconds.	F-41	Standard	Refined
PE-25	The statistics about usage of profiles should be presented to the administrator in less than 30 seconds.	F-42	Standard	
PE-26	Remote log-in should be performed in less than 60 seconds.	F-43	Critical	

PE-27	In case of an incomplete or unsuccessful command execution, an error response should be sent within 5 seconds	F-08	Standard	
PE-28	The used solutions for communication and system security shall be as much as possible lightweight to enforce in terms of performance, and especially feasible also for resource-constrained devices.	All	C	
PE-29	The performance impact due to communication and system security shall not result in unacceptable impact on the user experience.	All	C	
PE-30	The network infrastructure shall provide means also for one-to-many message delivery, e.g. over IP multicast.	F-47 F-48 F-49 F-50	C	
PE-31	It must be possible to have multiple security groups simultaneously active in the system.	F-47 F-48 F-49 F-50	C	
PE-32	When relevant, support shall be ensured for possible communication intermediaries performing, e.g., message forwarding and/or (transport-) protocol translation. This applies also in secure scenarios and also in (secure) group communication scenarios.	All	C	
PE-33	When relevant, it shall be possible to enable one-to-many response messages, sent at once to multiple requesters. This applies also to secure communication scenarios, and also in presence of communication intermediaries.	All	C	
PE-34	When relevant and limited to read-only operations, it shall be possible to enable cacheability of response messages at communication intermediaries, also when protected end-to-end.	All	C	
PE-35	Devices should, if available, utilize low-power modes of operation to further mitigate the performance impact of ongoing (D)DoS attacks.	All	S	
PE-36	There should be a means to enable an optimized, combined establishment of a cryptographic secret with a first message protected with key material derived from that secret.	All	S	
PE-37	In case of an incomplete or unsuccessful configuration change, an error message should be returned within 5 seconds	F-26	Standard	
RE-01	The system shall not fail more than once a week (in average).	All	Critical	Definition of "System failure" has been added to the glossary table
RE-02	The system shall not take more than one day to be repaired (in average).	All	Critical	
AV-01	The SIFIS-Home system services and devices shall be available 99% of the time	All	Critical	Refined
AV-02	The SIFIS-Home system shall ensure basic services availability in case of system failures.	All	Critical	Refined. A description is need of the SIFIS-Home system basic services and core functionalities required to be available 100% of the time - Adding definition of several failure levels.

AV-03	Support should be ensured for devices to dynamically react to (D)DoS attacks, by gradually adapting their availability. This includes relying on communication intermediaries for traffic offloading during intense (D)DoS attacks.	All	S	
AV-04	Devices under (D)DoS attacks should be able to continue providing a (best-effort) service to legitimate requests, i.e. by displaying a graceful degradation of quality of service.	All	S	
US-01	The system shall be easy to use for users with no technical background	All	Critical	Refined. This point of how to test this requirement and how to measure it needs to be explained
US-02	The SIFIS-Home system shall be autonomous and learn based on the users' habits, still according to defined privacy policies.	All	Critical	Refined
US-03	The SIFIS-Home system shall consider special cases in its design, such as colour blindness.	All	Optional	
US-04	The SIFIS-Home system shall preserve consistency among all devices, related database and constraints.	All	Critical	
US-05	The SIFIS-Home hardware components should be easy to use for the elderly and users with no engineering background.	All	Optional	
US-06	The SIFIS-Home system shall have an explorable interface.	All	Standard	
US-07	Proper and easy hardware installation should be considered.	All	Standard	
US-08	The image-based identification through biometrics in a room (interior) or in an open space (exterior), without obstacles or face covering elements, it should be performed by the system in a radius of at least 10 meters from the device.	F-01	Standard	
US-09	An untrained user should be able to understand that an attack is ongoing in less than a minute from reading the SIFIS-Home alert or notification.	F-09 F-13	Critical	1- Refined. 2- A description of the training is needed. 3- Definitions of "trained user" and "untrained user" have been added to the glossary table .
US-10	An untrained user should be able to recognise a software intrusion in less than one minute.	F-19 F-20	Critical	
US-11	An untrained user should be able to perform the device registration procedure in less than 5 minutes.	F-23	Standard	
US-12	An untrained user should be able to perform the device de-registration procedure in less than 5 minutes.	F-26	Standard	
US-13	An untrained user should be able to perform the configuration of devices in less than 5 minutes.	F-26	Standard	
US-14	An untrained user should be able to perform the installation of an application in less than 5 minutes.	F-28	Standard	
US-15	An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.	F-32	Standard	
US-16	An untrained user should be able to complete the configuration of policies for groups of devices in less than 5 minutes.	F-33	Standard	

US-17	An untrained user should be able to complete the configuration of profiles in less than 5 minutes.	F-37	Standard	
US-18	An untrained user should be able to perform a profile change in less than 30 seconds.	F-38	Standard	
US-19	An untrained user should be able to access the statistics for visualizing and interpreting them in less than 5 minutes.	F-41	Standard	Refined
US-20	The Multi-Level Anomaly Detection system (MLADS) must monitor network traffic provided by several input sources and several locations.	F-15 F-16 F-17 F-18	C	
US-21	The workload of the devices should be available to the MLADS.	F-15 F-16 F-17 F-18	C	
US-22	The list of applications running on each device should be available to MLADS.	F-15 F-16 F-17 F-18	C	
US-23	Raw sensor data must be available to be analysed by MLADS.	F-15 F-16 F-17 F-18	C	
US-24	Features from different devices should be aggregable directly or by means of pre-processing through specific analysis tools.	F-15 F-16 F-17 F-18	C	
US-25	When possible, a dataset should not be present as a whole on a single device for analysis.	All	S	
US-26	The presence of a GPU is needed to perform DL-based analysis.	F-15 F-16 F-17 F-18	S	
DE-01	The identification through biometrics should be performed correctly in more than 95% cases.	F-01	Critical	
DE-02	The start of an interaction command should be recognized properly and correctly in more than 99% of cases.	F-06	Critical	Refined
DE-03	The commands to execute should be recognized properly and correctly in more than 95% of cases.	F-06 F-07	Critical	Refined
DE-04	Record of intrusions must be available for a configurable time (default six months) after the recording.	F-10	Standard	Refined
DE-05	Identity of the successfully recognized intruders must be available for a configurable time (default six months) after the recording.	F-12	Standard	Refined
DE-06	Core functionalities should be replicated on multiple devices to avoid single points of failure.	F-21	Critical	A description of the SIFIS-Home system basic services and core

				functionalities like in AV-02 is needed
DE-07	The registration of a new device should be successful in at least 99% of the cases.	F-23	Critical	
DE-08	The de-registration of a new device should be successful in at least 99% of the cases	F-25	Critical	
DE-09	The configuration changes should be propagated successfully to the devices in more than 99% of times.	F-26	Critical	
DE-10	The SIFIS-Home system should be able to restore the previous configurations if there are errors in applying configuration changes.	F-26	Standard	Refined
DE-11	The installation of the selected app should be completed successfully in at least 95% of cases.	F-28	Critical	
DE-12	The application of policies should always be completed successfully.	F-31 F-34 F-33	Critical	Refined
DE-13	The configuration of profiles should be completed successfully in at least 99% of cases.	F-37	Critical	Assumptions are needed to be explained
DE-14	The change of current profile should be completed successfully in at least 99% of cases.	F-38	Critical	
DE-15	The statistics must be shown correctly in at least 99% of cases.	F-41	Critical	
DE-16	Remote log-in for the configurer should be successful in at least 99% cases.	F-43	Critical	
DE-17	The SIFIS-Home system should be able to distribute the processing among multiple machines in different places if required.	All	Critical	
DE-18	The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.	All	Critical	
DE-19	The SIFIS-Home system is required to be scalable dynamically by adding or removing nodes according to demand.	All	Critical	A description of system scalability is needed.
TE-01	The SIFIS-Home system needs Java version 8 or higher to interact with the ontology.		C	
TE-02	The process for getting and inserting information into the ontology will be through APIs provided via HTTP(S).		C	
TE-03	The software for handling the ontology should be hosted on a high-availability server.		C	
TE-04	Internet connectivity should be present.		S	

Table 7. Finalized list of Non-Functional requirements for the SIFIS-Home framework

Table 8 reports the list of original Non-Functional Requirements elicited for the SIFIS-Home system. Column "Feedback" summarizes the input provided by deliverables D3.1 and D4.1, that was taken into account to revise the requirements in the final requirements table of the present deliverable.The requirements to add according to deliverable D3.1 and D4.1 are reported at the end of the table.

Req. ID	Req. description	FR	Priority	Feedback
PE-01	The user authentication shall happen in less than 2s.	F-02 F-03	Critical	

PE-02	The user recognition (identification/ biometric-based) shall happen in less than 5s.	F-06	Critical	Refined
PE-03	Biometric-based authentication should be performed in less than 5 seconds.	F-03	Standard	
PE-04	Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.	F-04 F-05	Standard	"Activation of features" defined in a glossary table
PE-05	Recognition of the start of an interaction through voice command should be performed in less than 2 seconds.	F-06	Standard	
PE-06	The interpretation of the voice commands provided by the user should be performed in less than 2 seconds.	F-07	Standard	
PE-07	A command should be invoked within 5 seconds from the event that triggered its execution	F-08	Standard	Refined and a separate non-functional requirement has been added: "In case of an incomplete or unsuccessful command execution, an error response should be sent within 5 seconds"
PE-08	The maintainer must be able to access and watch a recording in less than one minute.	F-13	Standard	
PE-09	If requested to, the SIFIS-Home system shall contact law enforcement or private surveillance services to receive assistance in less than 30 seconds.	F-14	Optional	
PE-10	An abnormal (suspicious) behavior caused by a malware shall be identified and notified within 60 seconds	F-19	Optional	
PE-11	The user should be informed of the presence of a malware no later than 5 seconds after the malware is recognized.	F-20	Standard	Refined
PE-12	Self-healing algorithms should be started in less than 60 seconds if available when malware is recognized.	F-21	Critical	
PE-13	The registration of a new device should be completed in less than 30 seconds.	F-23	Standard	
PE-14	The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.	F-24	Standard	
PE-15	The de-registration of a device should be completed in less than 30 seconds.	F-25	Standard	
PE-16	The correct configuration changes should be propagated successfully in less than 30 seconds.	F-26	Critical	1- Refined. 2- Definition of "configuration" and "propagated successfully" have been added to the glossary table.

				3- A separate non-functional requirement has been added: "In case of an incomplete or unsuccessful configuration change, an error message should be returned within 5 seconds"
PE-17	The current configuration of a device should be retrieved in less than 10 seconds.	F-26	Standard	
PE-18	The marketplace should be accessible in less than 60 seconds.	F-28	Standard	Refined
PE-19	The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.	F-32	Critical	1- Refined 2- Definitions of "policy" and "user profile" have been added to the glossary table.
PE-20	The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.	F-33	Critical	Refined
PE-21	The list of policies should be retrieved in less than 30 seconds.	F-30	Standard	
PE-22	The configuration of profiles should be applied and enforced in less than 60 seconds.	F-37	Critical	Refined
PE-23	The change of current profile should be performed in less than 60 seconds.	F-38	Critical	Refined to consider "usage modes" instead of "profiles"
PE-24	The statistics about usage and behaviour of devices should be presented to the administrator in less than 30 seconds.	F-41	Standard	Refined
PE-25	The statistics about usage of profiles should be presented to the administrator in less than 30 seconds.	F-42	Standard	
PE-26	Remote log-in should be performed in less than 60 seconds.	F-43	Critical	
PE-27	In case of an incomplete or unsuccessful command execution, an error response should be sent within 5 seconds	F-08	Standard	
WP3 - PE-28	The used solutions for communication and system security shall be as much as possible lightweight to enforce in terms of performance, and especially feasible also for resource-constrained devices.	All	C	
WP3 - PE-29	The performance impact due to communication and system security shall not result in unacceptable impact on the user experience.	All	C	
WP3 - PE-30	The network infrastructure shall provide means also for one-to-many message delivery, e.g. over IP multicast.	F-47 F-48 F-49 F-50	C	
WP3 - PE-31	It must be possible to have multiple security groups simultaneously active in the system.	F-47 F-48 F-49	C	

		F-50		
WP3 - PE-32	When relevant, support shall be ensured for possible communication intermediaries performing, e.g., message forwarding and/or (transport-) protocol translation. This applies also in secure scenarios and also in (secure) group communication scenarios.	All	C	
WP3 - PE-33	When relevant, it shall be possible to enable one-to-many response messages, sent at once to multiple requesters. This applies also to secure communication scenarios, and also in presence of communication intermediaries.	All	C	
WP3 - PE-34	When relevant and limited to read-only operations, it shall be possible to enable cacheability of response messages at communication intermediaries, also when protected end-to-end.	All	C	
WP3 - PE-35	Devices should, if available, utilize low-power modes of operation to further mitigate the performance impact of ongoing (D)DoS attacks.	All	S	
WP3 - PE-36	There should be a means to enable an optimized, combined establishment of a cryptographic secret with a first message protected with key material derived from that secret.	All	S	
PE-37	In case of an incomplete or unsuccessful configuration change, an error message should be returned within 5 seconds	F-26	Standard	
RE-01	The system shall not fail more than once a week (in average).	All	Critical	Definition of "System failure" has been added to the glossary table
RE-02	The system shall not take more than one day to be repaired (in average).	All	Critical	
AV-01	The SIFIS-Home system services and devices shall be available 99% of the time	All	Critical	Refined
AV-02	The SIFIS-Home system shall ensure basic services availability in case of system failures.	All	Critical	Refined. A description is need of the SIFIS-Home system basic services and core functionalities required to be available 100% of the time - Adding definition of several failure levels.
WP3 - AV-03	Support should be ensured for devices to dynamically react to (D)DoS attacks, by gradually adapting their availability. This includes relying on communication intermediaries for traffic offloading during intense (D)DoS attacks.	All	S	
WP3 - AV-04	Devices under (D)DoS attacks should be able to continue providing a (best-effort) service to legitimate requests, i.e. by displaying a graceful degradation of quality of service.	All	S	
US-01	The system shall be easy to use for users with no technical background	All	Critical	Refined. This point of how to test this requirement and how to measure it needs to be explained

US-02	The SIFIS-Home system shall be autonomous and learn based on the users' habits, still according to defined privacy policies.	All	Critical	Refined
US-03	The SIFIS-Home system shall consider special cases in its design, such as colour blindness.	All	Optional	
US-04	The SIFIS-Home system shall preserve consistency among all devices, related database and constraints.	All	Critical	
US-05	The SIFIS-Home hardware components should be easy to use for the elderly and users with no engineering background.	All	Optional	
US-06	The SIFIS-Home system shall have an explorable interface.	All	Standard	
US-07	Proper and easy hardware installation should be considered.	All	Standard	
US-08	The image-based identification through biometrics in a room (interior) or in an open space (exterior), without obstacles or face covering elements, it should be performed by the system in a radius of at least 10 meters from the device.	F-01	Standard	
US-09	An untrained user should be able to understand that an attack is ongoing in less than a minute from reading the SIFIS-Home alert or notification.	F-09 F-13	Critical	1- Refined. 2- A description of the training is needed. 3- Definitions of "trained user" and "untrained user" have been added to the glossary table .
US-10	An untrained user should be able to recognise a software intrusion in less than one minute.	F-19 F-20	Critical	
US-11	An untrained user should be able to perform the device registration procedure in less than 5 minutes.	F-23	Standard	
US-12	An untrained user should be able to perform the device de-registration procedure in less than 5 minutes.	F-26	Standard	
US-13	An untrained user should be able to perform the configuration of devices in less than 5 minutes.	F-26	Standard	
US-14	An untrained user should be able to perform the installation of an application in less than 5 minutes.	F-28	Standard	
US-15	An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.	F-32	Standard	
US-16	An untrained user should be able to complete the configuration of policies for groups of devices in less than 5 minutes.	F-33	Standard	
US-17	An untrained user should be able to complete the configuration of profiles in less than 5 minutes.	F-37	Standard	
US-18	An untrained user should be able to perform a profile change in less than 30 seconds.	F-38	Standard	
US-19	An untrained user should be able to access the statistics for visualizing and interpreting them in less than 5 minutes.	F-41	Standard	Refined

DE-01	The identification through biometrics should be performed correctly in more than 95% cases.	F-01	Critical	
DE-02	The start of an interaction command should be recognized properly and correctly in more than 99% of cases.	F-06	Critical	Refined
DE-03	The commands to execute should be recognized properly and correctly in more than 95% of cases.	F-06 F-07	Critical	Refined
DE-04	Record of intrusions must be available for a configurable time (default six months) after the recording.	F-10	Standard	Refined
DE-05	Identity of the successfully recognized intruders must be available for a configurable time (default six months) after the recording.	F-12	Standard	Refined
DE-06	Core functionalities should be replicated on multiple devices to avoid single points of failure.	F-21	Critical	A description of the SIFIS-Home system basic services and core functionalities like in AV-02 is needed
DE-07	The registration of a new device should be successful in at least 99% of the cases.	F-23	Critical	Assumptions are needed to be explained
DE-08	The de-registration of a new device should be successful in at least 99% of the cases	F-25	Critical	Assumptions are needed to be explained
DE-09	The configuration changes should be propagated successfully to the devices in more than 99% of times.	F-26	Critical	Assumptions are needed to be explained
DE-10	The SIFIS-Home system should be able to restore the previous configurations if there are errors in applying configuration changes.	F-26	Standard	Refined
DE-11	The installation of the selected app should be completed successfully in at least 95% of cases.	F-28	Critical	Assumptions are needed to be explained
DE-12	The application of policies should always be completed successfully.	F-31 F-34 F-33	Critical	Refined
DE-13	The configuration of profiles should be completed successfully in at least 99% of cases.	F-37	Critical	Assumptions are needed to be explained
DE-14	The change of current profile should be completed successfully in at least 99% of cases.	F-38	Critical	Assumptions are needed to be explained
DE-15	The statistics must be shown correctly in at least 99% of cases.	F-41	Critical	
DE-16	Remote log-in for the configurer should be successful in at least 99% cases.	F-43	Critical	Assumptions are needed to be explained
DE-17	The SIFIS-Home system should be able to distribute the processing among multiple machines in different places if required.	All	Critical	
DE-18	The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.	All	Critical	
DE-19	The SIFIS-Home system is required to be scalable dynamically by adding or removing nodes according to demand.	All	Critical	A description of system scalability is needed.
WP4-US-01	The Multi-Level Anomaly Detection system (MLADS) must monitor network traffic provided by several input sources and several locations.	F-15 F-16 F-17	C	

		F-18		
WP4-US-02	The workload of the devices should be available to the MLADS.	F-15	C	
		F-16		
		F-17		
		F-18		
WP4-US-03	The list of applications running on each device should be available to MLADS.	F-15	C	
		F-16		
		F-17		
		F-18		
WP4-US-04	Raw sensor data must be available to be analysed by MLADS.	F-15	C	
		F-16		
		F-17		
		F-18		
WP4-US-05	Features from different devices should be aggregable directly or by means of pre-processing through specific analysis tools.	F-15	C	
		F-16		
		F-17		
		F-18		
WP4-US-06	When possible, a dataset should not be present as a whole on a single device for analysis.	All	S	
WP4-US-07	The presence of a GPU is needed to perform DL-based analysis.	F-15	S	
		F-16		
		F-17		
		F-18		
WP4-TE-01	The SIFIS-Home system needs Java version 8 or higher to interact with the ontology.		C	
WP4-TE-02	The process for getting and inserting information into the ontology will be through APIs provided via HTTP(S).		C	
WP4-TE-03	The software for handling the ontology should be hosted on a high-availability server.		C	
WP4-TE-04	Internet connectivity should be present.		S	

Table 8. Comments to the initial set of non-functional requirements

5.3 *Security Requirements*

Security requirements are a specific set of non-functional requirements which do not directly derive from specific functional requirements. Security requirements derive instead from laws and regulations, security standards, protocols and best practices. To discuss the security requirements, we will refer to the Open Security Architecture (OSA) standard to describe security requirements, dividing them into:

Testable Security Requirements (TSR) are security-related functions that the system must be able to perform. These requirements are testable, so one should be able to create test cases for them.

Non-Testable Security Requirements (NTSR) cannot be tested to be either working or not in a black-and-white fashion, but they can be measured by using metrics. Non-testable security requirements are of two sub-classes: one-time and continuous security requirements. One-time security requirements are implemented within a system and tested to ensure that they are fulfilled. For example, user passwords are hashed is such a way as to protect systems against rainbow table attacks. Continuous security requirements are constraints on other requirements and may influence the system at any time. These include, for example, the validation of parameters in a HTTP POST request.

Table 9 distinguishes and summarises the characteristics of and the differences between TSR and NTSR, whereas Figure 12 connects the sources of security requirements with TSR and NTSR.

Security requirements				
Type	**Describes**	**Derived from**	**Example**	**Validation**
TSR	Security services that the system has to provide.	Best practices, Policies, Regulations	Application X has to be possible to use only with user rights given by an administrator.	Testable
NTSR • One-time • Continuous	Architectural security requirements.	Architectural principals, Good practice, Standards	Availability, Integrity, Confidentiality	Measurable

Table 9. Characteristics of TSR and NTSR

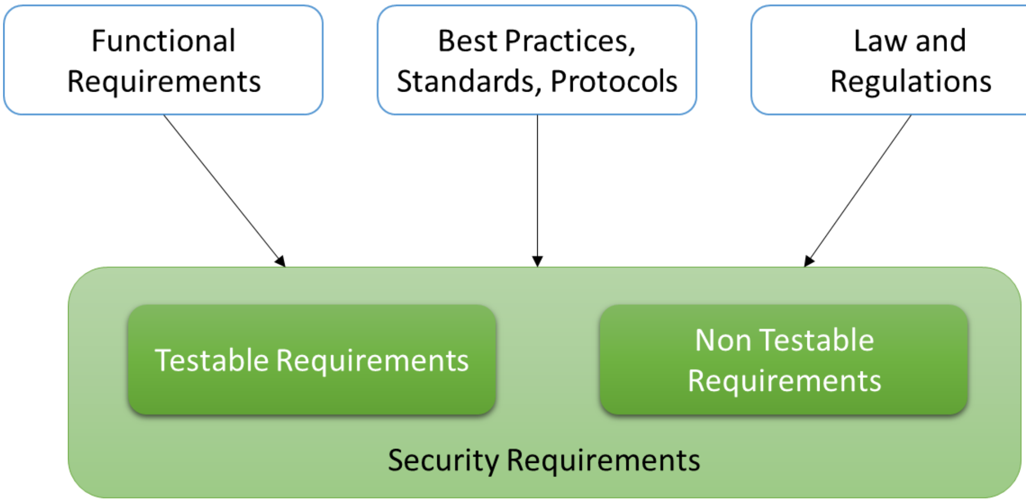


Figure 12. Security Requirements Gathering

Requirements coming from standards and protocols are generally intended to fulfil the standard objectives of security, namely:

- **Confidentiality** is the property by which unauthorized users do not have access to information.
- **Integrity** is the property by which information cannot be unnoticeably modified or destructed by unauthorized users, and information completeness and accuracy is maintained all over the information life cycle.
- **Availability** in information systems is the property by which information and services have to be available when needed and requested. Consequently, security controls are used to protect information systems from service disruptions. Security controls also ensures high technical reliability of the communication channels.

From these basic security objectives should be derived also those requirements related to system *dependability*, management of *access control*, *authentication* and *authorisation*. Law and regulations requirements mainly derive from GDPR and the NIST regulation on data management, which provide requirements related to management and storage of data. In the SIFIS-Home project, a deep analysis of these requirements is performed in Task 2.4. A particular attention for what concerns these requirements is dedicated to users' data privacy, in order to empower the user with a complete control on the data produced and collected by the framework and by supporting the development of analytics services which are privacy preserving and based on the minimum needed privilege paradigm.

In Table 10, we report the requirements after the refinement that took into account the comments on the requirements provided by deliverables D3.1 and D4.1, and Tthe requirements to add according to deliverable D3.1 and D4.1 are reported at the end of the table.

Req ID	Requirement Description.	FR	Testable	Priority	Feedback
SE-01	APIs for the communication with internal devices must be secured.	C-02	NT	Critical	O
SE-02	APIs for the communication with external devices must be secured.	C-04	NT	Critical	O
SE-03	Personal data stored must be encrypted.	F-49 F-56 S-04	T	Critical	O
SE-04	The system shall protect and avoid disclosure of sensitive information.	F-56 F-62 S-04	NT	Critical	O
SE-05	The SIFIS-Home system shall prevent data alteration or deletion.	F-56 F-61 S-04	NT	Critical	O
SE-06	Wifi access should be protected against known WiFi security attacks.	C-01 C-03	T	Critical	O
SE-07	Biometrics must be stored safely in the SIFIS-Home database.	F-03	NT	Critical	O
SE-08	Log-in information should be stored in a protected database.	F-62	NT	Critical	O
SE-09	The information about the registered devices, their characteristics and their configurations should be stored in a protected database.	F-25 F-38 F-44	NT	Critical	O
SE-10	The information about policies should be stored in a protected database.	F-33	NT	Critical	O
SE-11	The information about user profiles and configuration aspects should be stored in a protected database.	F-39 F-42 F-44	NT	Critical	O
SE-12	Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.	General	T	Critical	A
SE-13	Data confidentiality shall be ensured all the time.	General	NT	Critical	A
SE-14	The system should not be affected by MITM attacks.	General	T	Critical	R
SE-15	Software and apps shall only be installed with authorisation of the smart home administrator or resident users.	General	T	Critical	R
SE-16	Users must be able to configure and allow the usage of data to~~by~~ the SIFIS-Home framework and third- party software.	General	T	Critical	A/R
SE-17	Anomalous device behaviours should be identified and signalled in less than 60 seconds.	General	T	Critical	R
SE-18	Minimum needed privilege principle must always be enforced.	General	NT	Critical	A

SE-19	Access to device~~s~~ functionalities should be protected and controlled	General	NT	Critical	A
SE-20	Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.	General	NT	Critical	A
SE-21	Privacy preferences shall be configurable for data, analytics and functionalities.	General	NT	Critical	A
SE-22	Analytics shall be able to work with anonymized data when possible.	General	NT	Critical	O
SE-23	The SIFIS-Home architecture shall be resilient to network-based attacks.	General	T	Critical	R
SE-24	The SIFIS-Home architecture shall be resilient to DoS attacks.	General	T	Critical	R
SE-25	The SIFIS-Home architecture shall be resilient to sybil attacks.	General	T	Critical	R
SE-26	The SIFIS-Home architecture shall be resilient to device compromising attacks.	General	T	Critical	R
SE-27	The SIFIS-Home architecture shall be resilient to Internet connection failure.	General	T	Critical	R
SE-28	The SIFIS-Home architecture shall be resilient to physical device damage or failure.	General	T	Critical	R
SE-29	Devices must have unique identifiers.	General	NT	Critical	R
SE-30	Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.	General	T	C	
SE-31	It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.	General	T	C	
SE-32	It shall be possible to achieve end-to-end protection of CoAP messages at the application layer, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection. This applies also in case communication intermediaries are used, as well as for both one-to-one and one-to-many (group) communication.	General	T	C	
SE-33	Cryptographic binding between a protected request message and one or many corresponding protected response(s) shall be ensured.	General	T	C	
SE-34	Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.	General	T	C	
SE-35	Cryptoagility shall be ensured, as a way to allow a seamless possible switch to different existing algorithms as well as a seamless possible migration to future algorithms.	General	T	C	
SE-36	Operations related to the creation, configuration, deletion, registration and discovery of security groups shall be secured and shall be allowed only to authorized entities.	F-23	T	C	
		F-25			
		F-26			
		F-30			
		F-31			
		F-32			
		F-33			
		F-34			
		F-35			
		F-47			

		F-48 F-49			
SE-37	When relevant, it shall be ensured that a possible communication intermediary can securely identify its adjacent communication hops.	General	T	C	
SE-38	It shall be ensured that possible secure cacheable response messages do not break security properties that are critical for the application and specific communication exchanges.	General	T	C	
SE-39	Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.	General	NT	S	
SE-40	The system shall provide a means to enforce flexible, fine-grained and reactive authorized access control for devices to access remote resources at other devices.	General	T	C	
SE-41	It shall be possible to establish security material to use for end-to-end secure (group) communication in an authorized way, achieving confirmation of the established material.	General	T	C	
SE-42	The system shall provide a means for enabling devices to get agile and possibly automatic notification, in order to signal pertaining access credentials that have been revoked while still unexpired.	General	T	C	
SE-43	There shall be means for two devices to securely establish a new cryptographic secret with perfect forward secrecy, while also achieving mutual authentication and confirmation of the established material.	General	T	C	
SE-44	There shall be an authorization-based means to securely join/leave a security group and retrieve/provide updated key material to communicate in the group.	F-23 F-25 F-26 F-30 F-31 F-32 F-33 F-34 F-35 F-50	T	C	
SE-45	There shall be a means to securely renew the key material in a security group, both periodically and in case the application requires backward/forward security.	F-19 F-23 F-25 F-26 F-50	T	C	
SE-46	When limits on usage of cryptographic material for encryption and decryption are exceeded, devices owning that key material shall stop using it and specific actions shall be taken to acquire new material before possibly resuming communication. The just invalidated key material may be temporarily retained and used only for processing incoming messages for a limited, pre-configured amount of time.	General	T	C	
SE-47	There shall be a means for two devices to securely update their pairwise key material.	General	T	C	
SE-48	Device administrable domain should be known.	all	n	S	
SE-49	Definition of a template for each type of device which describes the features of the specific type of device.	all	n	S	

SE-50	The identity of the speaker should not be identifiable if the analysis is outsourced to external services.	UC-02	n	S	
SE-51	The background noises in the audio streams must be anonymized if the analysis is outsourced to external services.	UC-02	n	S	
SE-52	Personal information recognizable from audio (e.g., name, telephone number, email address, age, physical condition) must be anonymized if the analysis is outsourced to external services.	UC-02	n	S	

Table 10. Final list of elicited security requirements

Table 11 lists the original elicited security requirements for the SIFIS-Home system. For the prioritisation of these security requirements, the same notation already used for functional and non-functional requirement is used. The requirements to add according to deliverable D3.1 and D4.1 are reported at the end of the table.

Req ID	Requirement Description.	FR	Testable	Priority	Feedback
SE-01	APIs for the communication with internal devices must be secured.	C-02	NT	Critical	O
SE-02	APIs for the communication with external devices must be secured.	C-04	NT	Critical	O
SE-03	Personal data stored must be encrypted.	F-49 F-56 S-04	T	Critical	O
SE-04	The system shall protect and avoid disclosure of sensitive information.	F-56 F-62 S-04	NT	Critical	O
SE-05	The SIFIS-Home system shall prevent data alteration or deletion.	F-56 F-61 S-04	NT	Critical	O
SE-06	Wifi access should be protected against known WiFi security attacks.	C-01 C-03	T	Critical	O
SE-07	Biometrics must be stored safely in the SIFIS-Home database.	F-03	NT	Critical	O
SE-08	Log-in information should be stored in a protected database.	F-62	NT	Critical	O
SE-09	The information about the registered devices, their characteristics and their configurations should be stored in a protected database.	F-25 F-38 F-44	NT	Critical	O
SE-10	The information about policies should be stored in a protected database.	F-33	NT	Critical	O
SE-11	The information about user profiles and configuration aspects should be stored in a protected database.	F-39 F-42 F-44	NT	Critical	O
SE-12	Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.	General	T	Critical	A
SE-13	Data confidentiality shall be ensured all the time.	General	NT	Critical	A
SE-14	The system should not be affected by MITM attacks.	General	T	Critical	R
SE-15	Software and apps shall only be installed with authorisation of the smart home administrator or resident users.	General	T	Critical	R

SE-16	Users must be able to configure and allow the usage of data to~~by~~ the SIFIS-Home framework and third- party software.	General	T	Critical	A/R
SE-17	Anomalous device behaviours should be identified and signalled in less than 60 seconds.	General	T	Critical	R
SE-18	Minimum needed privilege principle must always be enforced.	General	NT	Critical	A
SE-19	Access to device~~s~~ functionalities should be protected and controlled	General	NT	Critical	A
SE-20	Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.	General	NT	Critical	A
SE-21	Privacy preferences shall be configurable for data, analytics and functionalities.	General	NT	Critical	A
SE-22	Analytics shall be able to work with anonymized data when possible.	General	NT	Critical	O
SE-23	The SIFIS-Home architecture shall be resilient to network-based attacks.	General	T	Critical	R
SE-24	The SIFIS-Home architecture shall be resilient to DoS attacks.	General	T	Critical	R
SE-25	The SIFIS-Home architecture shall be resilient to sybil attacks.	General	T	Critical	R
SE-26	The SIFIS-Home architecture shall be resilient to device compromising attacks.	General	T	Critical	R
SE-27	The SIFIS-Home architecture shall be resilient to Internet connection failure.	General	T	Critical	R
SE-28	The SIFIS-Home architecture shall be resilient to physical device damage or failure.	General	T	Critical	R
SE-29	Devices must have unique identifiers.	General	NT	Critical	R
WP3 - SE-30	Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.	General	T	C	
WP3 - SE-31	It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.	General	T	C	
WP3 - SE-32	It shall be possible to achieve end-to-end protection of CoAP messages at the application layer, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection. This applies also in case communication intermediaries are used, as well as for both one-to-one and one-to-many (group) communication.	General	T	C	
WP3 - SE-33	Cryptographic binding between a protected request message and one or many corresponding protected response(s) shall be ensured.	General	T	C	
WP3 - SE-34	Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.	General	T	C	
WP3 - SE-35	Cryptoagility shall be ensured, as a way to allow a seamless possible switch to different existing algorithms as well as a seamless possible migration to future algorithms.	General	T	C	
WP3 - SE-36	Operations related to the creation, configuration, deletion, registration and discovery of security groups shall be secured and shall be allowed only to authorized entities.	F-23 F-25 F-26 F-30 F-31 F-32	T	C	

		F-33 F-34 F-35 F-47 F-48 F-49			
WP3 - SE-37	When relevant, it shall be ensured that a possible communication intermediary can securely identify its adjacent communication hops.	General	T	C	
WP3 - SE-38	It shall be ensured that possible secure cacheable response messages do not break security properties that are critical for the application and specific communication exchanges.	General	T	C	
WP3 - SE-39	Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.	General	NT	S	
WP3 - SE-40	The system shall provide a means to enforce flexible, fine-grained and reactive authorized access control for devices to access remote resources at other devices.	General	T	C	
WP3 - SE-41	It shall be possible to establish security material to use for end-to-end secure (group) communication in an authorized way, achieving confirmation of the established material.	General	T	C	
WP3 - SE-42	The system shall provide a means for enabling devices to get agile and possibly automatic notification, in order to signal pertaining access credentials that have been revoked while still unexpired.	General	T	C	
WP3 - SE-43	There shall be means for two devices to securely establish a new cryptographic secret with perfect forward secrecy, while also achieving mutual authentication and confirmation of the established material.	General	T	C	
WP3 - SE-44	There shall be an authorization-based means to securely join/leave a security group and retrieve/provide updated key material to communicate in the group.	F-23 F-25 F-26 F-30 F-31 F-32 F-33 F-34 F-35 F-50	T	C	
WP3 - SE-45	There shall be a means to securely renew the key material in a security group, both periodically and in case the application requires backward/forward security.	F-19 F-23 F-25 F-26 F-50	T	C	
WP3 - SE-46	When limits on usage of cryptographic material for encryption and decryption are exceeded, devices owning that key material shall stop using it and specific actions shall be taken to acquire new material before possibly resuming communication. The just invalidated key material may be temporarily retained and used only for processing incoming messages for a limited, pre-configured amount of time.	General	T	C	

WP3 - SE-47	There shall be a means for two devices to securely update their pairwise key material.	General	T	C	
WP4-SE-01	Device administrable domain should be known.	all	n	S	
WP4-SE-02	Definition of a template for each type of device which describes the features of the specific type of device.	all	n	S	
WP4-SE-03	The identity of the speaker should not be identifiable if the analysis is outsourced to external services.	UC-02	n	S	
WP4-SE-04	The background noises in the audio streams must be anonymized if the analysis is outsourced to external services.	UC-02	n	S	
WP4-SE-05	Personal information recognizable from audio (e.g., name, telephone number, email address, age, physical condition) must be anonymized if the analysis is outsourced to external services.	UC-02	n	S	

Table 11. A list of elicited security requirements for the SIFIS-Home system

5.4 *Mapping of Requirements on Use Cases*

Table 12 gives a visual representation and summary of the mapping of the functional requirements defined in the previous section to the use cases that were used to generate them.

	SIFIS-UC-1	SIFIS-UC-2	SIFIS-UC-3	SIFIS-UC-4	SIFIS-UC-5	SIFIS-UC-6	SIFIS-UC-7	SIFIS-UC-8	SIFIS-UC-9	SIFIS-UC-10	SIFIS-UC-11	SIFIS-UC-12	SIFIS-UC-13	SIFIS-UC-14
F-01	x													
F-02	x													
F-03	x													
F-04	x													
F-05	x													
F-06	x		x											
F-07		x												
F-08		x												
F-09		x												
F-10			x											
F-11			x											x
F-12			x											x
F-13			x											x
F-14			x											x
F-15			x											x
F-16			x											x
F-17			x											x
F-18			x											x
F-19				x										
F-20				x										
F-21				x										
F-22				x										
F-23					x									
F-24					x	x	x					x		
F-25						x						x		
F-26							x							
F-27							x					x		
F-28								x						
F-29								x						
F-30									x				x	
F-31									x				x	

F-32									x				x	
F-33									x				x	
F-34									x				x	
F-35									x				x	
F-36										x				
F-37										x				
F-38										x				
F-39										x				
F-40										x				
F-41											x			
F-42											x			
F-43												x	x	
F-44													x	
F-45														x
F-46										x				

Table 12. Mapping of Requirements to Use Cases

6 Evaluation and Validation

The validation will be based on the acceptance tests defined for each use case. In particular, for each defined acceptance test, the activities of WP5 and WP6 will verify if the functionalities of the framework are able to pass or not the test. Specific acceptance tests will also be defined for the security testable requirements.

To formally evaluate and validate the collected requirements, we adopt the Goal Question Metric (GQM) approach, originally proposed by Victor Basili [Basili, 1994] as a measurement mechanism for feedback and evaluation in Software Engineering. The GQM can be applied to any deliverable of the software engineering and development lifecycle, e.g. specifications, design, programs, and test suites, but also to processes involved in the development.

The GQM template is divided in three levels:

- Conceptual Level (the *goal*): defines what the object of improvement or evaluation is. The goal can be further decomposed into five different fields:
    - *Analyse* {the name of activity or attribute}
    - *For the purpose of* {overall goal}
    - *With respect to* {the aspect to be considered}
    - *From the viewpoint of* {interested people}
    - *In the context of* {environment}
- Operational Level (the *question*): defines one or more questions, to characterize the way the assessment/achievement of a specific goal is going to be performed.
- Quantitative Level (the *metric*): a set of data is associated with every question, in order to answer it in a quantitative way. The data can be objective, if they depend only on the object that is being measured and not on the viewpoint from which they are taken; or subjective, if they depend on both the object that is being measured and the view point from which they are taken.

Several advantages provided by the GQM approach are reported in the Software Engineering literature. It helps to ensure adequacy, consistency, and completeness of the measurement plans deployed and of data collection, and to manage the complexity of the measurement program.

It is foreseen to adopt the Goal Question Metric template to assess the quantity of Functional and Non-Functional Requirements successfully implemented at the end of the development phases of the project. The GQM conceptual table is reported in Table 13.

Analyze	The results of Acceptance tests
For the purpose of	Evaluation and validation of the current state of the system
With respect to	Functional and Non-functional requirements
From the viewpoint of	Developers, Testers
In the context of	SIFIS-Home system

Table 13. GQM conceptual table

The GQM template will include boolean variables to assess the implementation of each individual Functional Requirement, gathered after execution of the related acceptance tests. Specific metrics will be defined for each Non-Functional Requirements (e.g., response time for performance-related Non-Functional Requirements), to give a quantitative assessment of the coverage provided by the implementation.

In Table 14, a subset of the final GQM table is reported. The *questions* are categorized according to the type of requirements they are designed to assess. Each row of the table reports the type of metric to answer the question, and the measurements for the metric at each assessment period of the project. We foresee at least three assessments for each question: at M24, in occasion of the first release of the SIFIS-Home implementation; at M33, in occasion of the final testbed validation; at M36, in occasion of the pilot validation.

Req. Ref	Type	Question	Metric	Measure at M24	Measure at M33	Measure at M36
FR-01	Assessment of individual Functional Requirement assessment	Can the users be identified through biometrics (e.g., face, fingerprint)?	Boolean			
PE-01	Assessment of individual Non-Functional Requirement	How many functional requirements have been successfully implemented?	Boolean			
SE-01	Assessment of individual Non-Functional Requirement	How long does it take to perform user authentication?	Integer (seconds)			
FR-01/46	Aggregate assessment of a category of requirements	Are APIs for communications with external devices secured?	Integer			

Table 14. An illustration of a subset of the final GQM table

7 Conclusion

In this deliverable we have extended the work done in D1.1 to gather functional, non-functional and security requirements for the SIFIS-Home framework. This deliverable has condensed the activities of Task 1.1 and Task 1.2, which are related to a background study of techniques for requirement gathering as well as the rationale behind the selection of a specific methodology. We have considered the feedbacks received from D3.1 and D4.1, as well as input and comments of requirements coming from the initial architecture definition which is presented in D1.3. A set of seven user stories has been defined, from which we have extracted 14 use cases together with their acceptance tests. Finally, the sets of functional, non-functional and security requirements have been presented.

8 References

[Basili, 1994] Basili, Victor R. "Goal question metric paradigm." Encyclopedia of software engineering (1994): 528-532.

[Cockburn, 1998] Cockburn, A. (1998). Use Case Template. CU-Boulder: Computer Science.

[Cohn, 2004] Cohn, M. (2004). Advantages of user stories for requirements. InformIT Network, available at: http://www. informit. com/articles.

[Crespi, 2008] Crespi, V., Galstyan, A., & Lerman, K. (2008). Top-down vs bottom-up methodologies in multi-agent system design. Autonomous Robots, 24(3), 303-313.

[Jacobson, 2004] Jacobson, I. (2004). Use cases–Yesterday, today, and tomorrow. Software & Systems Modelling, 3(3), 210-220.

[Leffingwell, 2010] Leffingwell, D. (2010). Agile software requirements: lean requirements practices for teams, programs, and the enterprise. Addison-Wesley Professional.

[Sharp, 1999] Sharp, H., Finkelstein, A., & Galal, G. (1999, September). Stakeholder identification in the requirements engineering process. In Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99 (pp. 387-391). Ieee.

Glossary

Acronym	Definition
DHT	Distributed Hash Table
FR	Functional Requirements
NFR	Non-functional requirement
OS	Operative System
P2P	Peer to Peer
SIFIS-Home	Secure Interoperable Full Stack Internet of Things for Smart Home
UC	Use case
US	User story
SD	Smart Device
NSSD	Not So Smart Device

Table 15. List of Acronyms

Term	Description
Activation of features	To activate specific services and functionalities based on the identity of the user
propagated successfully	Pushing and distributing changes among services and devices
configuration	An arrangement of components in a system such as policies
policy	A system rule that overrides user settings and defines available resources to a user or a group of users
user profile	A collection of information and settings associated with a specific user
System failure	A hardware or software problem that causes the system to end abnormally
Trained User	A user that has received full training materials and done a self-instruction training for SIFS-Home System.
Untrained User	A user that did not receive the training material or did not finish the SIFIS-Home system self-instruction training.
Processing	analysis methods applied on data collected from smart home devices
System Scalability	The system's ability to increase and decrease its performance in response to changes in network and applications

Table 16. List of SIFIS-Home specific terms