D6.3

Refined Pilot Use Case Requirements

WP6 – Smart Home Pilot Use Case

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/03/2023
Actual submission date: 31/03/2023

Responsible partner: DOMO
Editor: Domenico De Guglielmo;
E-mail address: domenico.deguglielmo@domo-iot.com

30/03/2023
Version 1.0

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

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

Authors: Domenico De Guglielmo (DOMO), Andrea Saracino (CNR), Riccardo Coppola (POLITO)

Approved by: Håkan Lundström (SEN), Marko Komssi (FSEC)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	15/02/2023	Defined ToC	DOMO	All
0.2	18/02/2023	Updated list of devices	DOMO	1
0.3	07/03/2023	Final list of use cases defined	DOMO, CNR, POLITO	2, 3
0.4	09/03/2023	Functional requirements list updated. Defined GQM questions.	DOMO, CNR, POLITO	3
0.5	21/03/2023	Internal review completed	SEN, FSEC	All
1	23/03/2023	Final version	DOMO	All

Executive Summary

This deliverable reports the final list of smart home use cases that are going to be implemented, validated and tested using the SIFIS-Home pilot implementation. For every use case, an End-to-End (E2E) acceptance test is reported as well as details about how we plan to implement and test the use case in the pilot. Also, a set of GQM (Goal, Quality and Metrics [GQM]) questions is reported for every use case. The tests we plan to perform will allow to verify the feasibility of the SIFIS-Home framework for the home automation scenario. This deliverable deprecates D6.1.

Table of contents

Contents

1 Introduction

This deliverable reports the final list of the smart home use cases that will be demonstrated and tested using the SIFIS-Home project pilot. The structure of the deliverable is as follows. First, we provide a detailed overview of the different devices that we are going to use in the pilot highlighting their type (e.g. Smart Device (SD) or Not So Smart Devices (NSSD)). Then, we describe all the different smart home use cases that we considered and report the list of tests that we plan to perform to verify that the requirements of the use cases are satisfied by the final pilot implementation.

2 Devices used in the pilot

This section describes the different smart (SD) and not-so-smart (NSSD) devices that are used in the current pilot implementation. The main hardware characteristics of the various devices are reported and their specific use in the pilot is highlighted.

2.1 *Smart Devices*

Smart devices are powerful devices where it is possible to install a number of applications. They execute the set of SIFIS-Home software components that compose the SIFIS-Home Smart Device framework. In the following we describe the smart devices that are currently used in the pilot.

2.1.1 DoMO gateway

Figure 1 shows the DoMO gateway, i.e. the main smart device used in our pilot. The DoMO gateway is a quite powerful device, based on the Banana PI R3 board [BANANA PI], that is provided with a Quad Core ARM A53 CPU and 2 GB of DDR RAM. Also, it has 8GB of EMMC flash available. Regarding network connectivity, the DoMO gateway is equipped with two 4x4 Wi-Fi 6 network chips (2.4Ghz and 5Ghz bands), 5 Gb Ethernet ports and 2 2.5 Gb SFP ports. Also, it is provided with a user-accessible USB 3.0 compliant port that allows connecting external USB devices. Additional details of the device are reported in Figure 2.

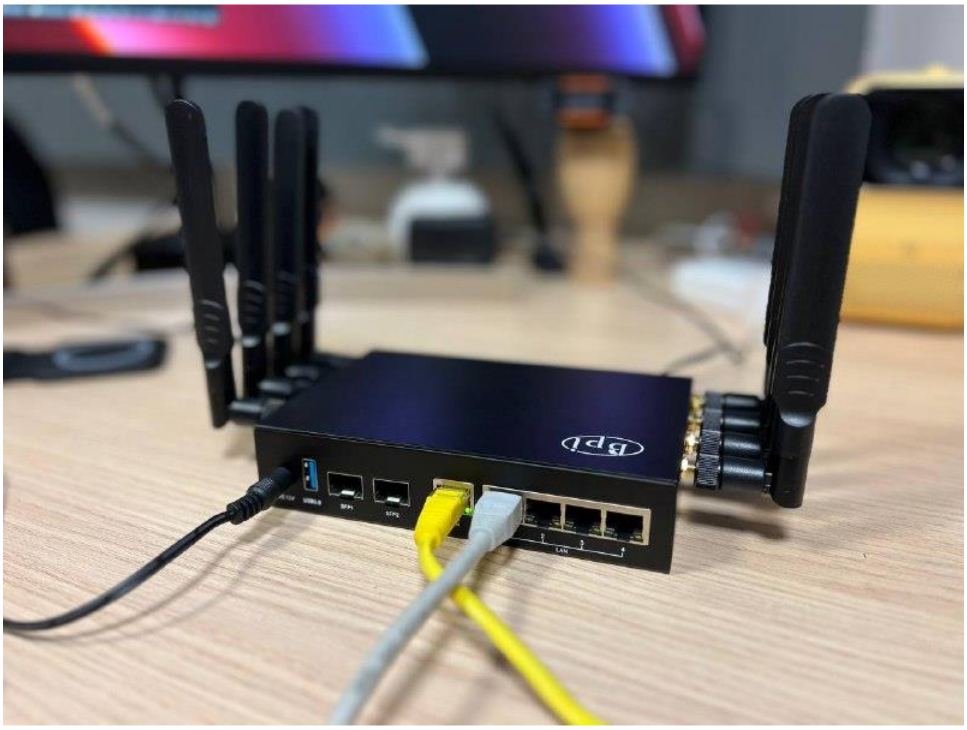

Figure 1: Domo Gateway

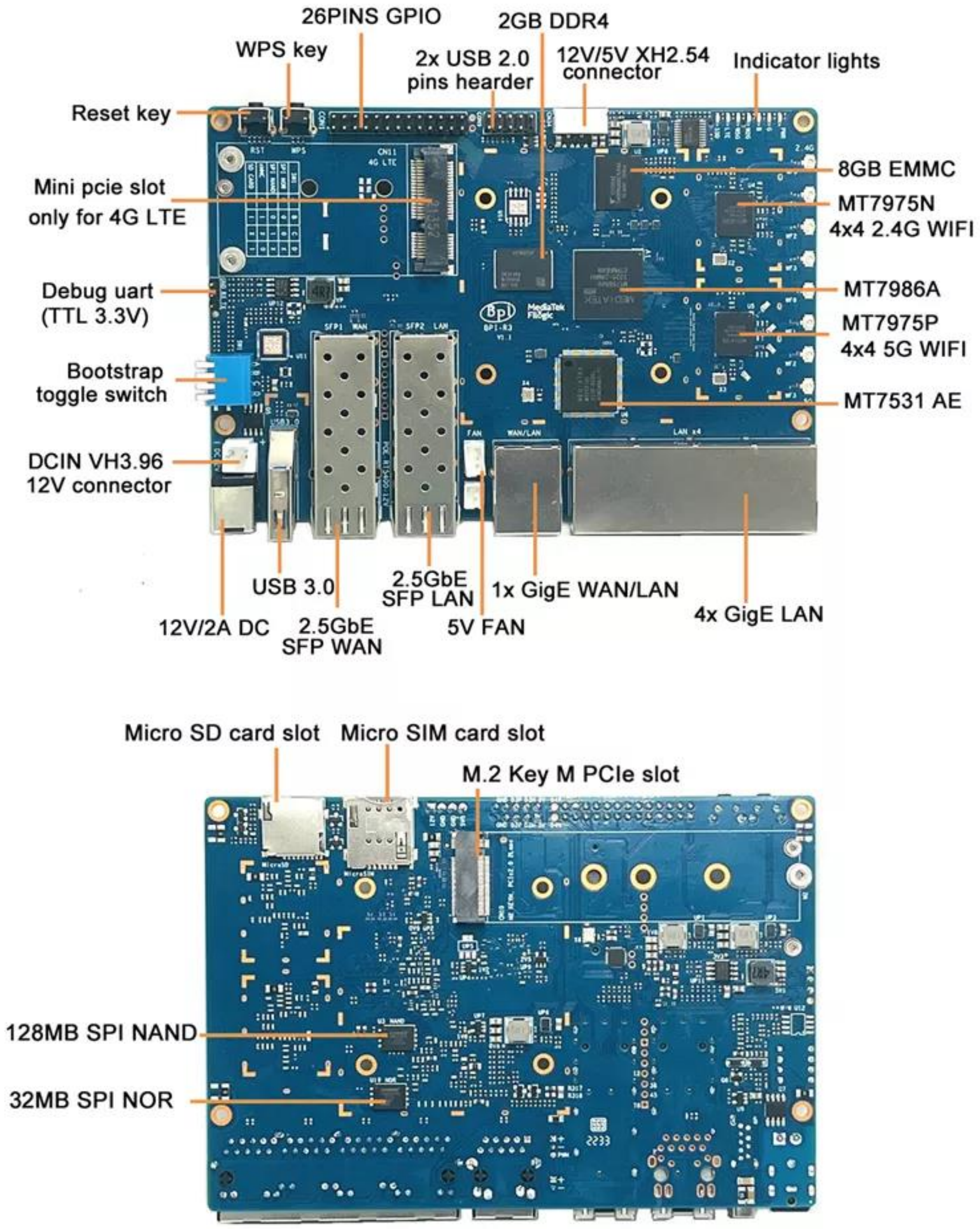

Figure 2: Domo Gateway details

2.1.2 Raspberry PI 4, Model B

We are currently using Raspberry Pi 4 model B [RASPBERRY PI] devices in the pilot. They have 4 GB of RAM available and run a 64-bit version of the Raspberry Pi OS.

2.1.3 Laptop

We plan to use a number of x86 laptops in the pilot. Our intention is to use them to run applications that are computationally intensive and, hence, cannot be executed on the SME partner smart devices due to their limited memory and performance.

2.1.4 Smartphone

Smartphones are the devices that run the SIFIS-Home mobile application. They are mainly used to test the UI components of the SIFIS-Home Mobile Application Framework and allow the user to interact with the smart home.

2.2 *Not So Smart Devices*

Not so smart devices are small, constrained devices that are mainly used to interact with the physical world. We report the details of the NSSDs used in the pilot in the following section.

2.2.1 DoMO Wi-Fi actuators

The SIFIS-Home pilot uses different types of Wi-Fi actuators [SHELLY], provided by DoMO, to control and monitor the energy consumption of the lights, sockets, shutters and appliances installed inside the house. The Wi-Fi actuators are simple devices that provide output and input channels and allow to turn on and off the appliances/light/sockets they are attached to as well as measure and report their energy consumption. Using the input channels of the actuators it is also possible to detect the state of attached buttons and bistable buttons as well as the state of attached window and door contact sensors. All the actuators are equipped with an Espressif ESP8266 Wi-Fi chip that can be flashed with a custom firmware.

In the following we briefly describe the characteristics of the various types of Wi-Fi actuators that are used in the pilot.

Shelly 1
Figure 3 shows the Shelly 1 Wi-Fi actuator. It provides one input channel and a potential-free output channel. It is not provided with an energy monitoring chip. It can be used to turn on and off lights and appliances as well as heating systems. Also, it can detect state changes of buttons/contacts to which its input channel is connected to.

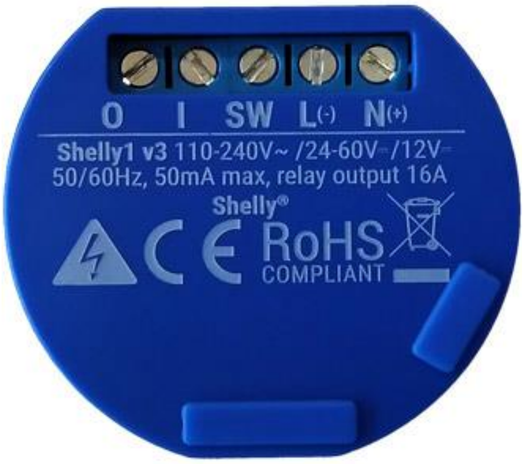
O I SW L(-) N(+)
Shelly1 v3 110-240V~ /24-60V⎓ /12V⎓
50/60Hz, 50mA max, relay output 16A
Shelly®
CE RoHS COMPLIANT

Figure 3: Shelly 1

Shelly 1PM
Figure 4 shows the Shelly 1PM Wi-Fi actuator. It provides one input channel and one output channel. It can be used to turn on and off lights and appliances and monitor their energy consumption. Also, it can detect state changes of buttons/contacts to which its input channel is connected to.

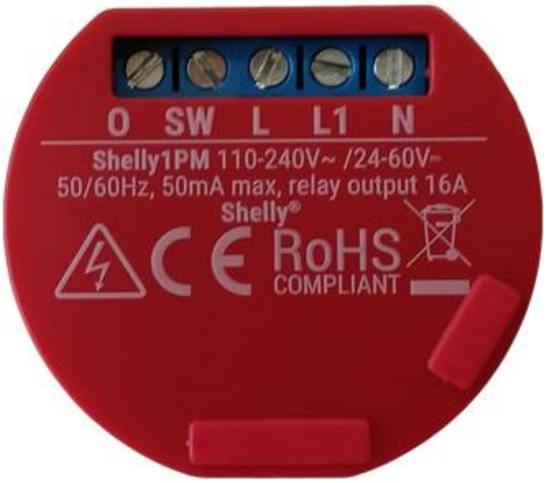
O SW L L1 N
Shelly1PM 110-240V~ /24-60V⎓
50/60Hz, 50mA max, relay output 16A
Shelly®
RoHS
COMPLIANT

Figure 4: Shelly 1PM

Shelly 2.5
Figure 5 shows the Shelly 2.5 Wi-Fi actuator. It provides two input channels and two output channels. It can be used to turn on and off light and appliances and monitor their energy consumption. Also, it allows to open/close shutters and curtains. Finally, it can detect changes in the state of buttons/contacts to which its input channels are attached.

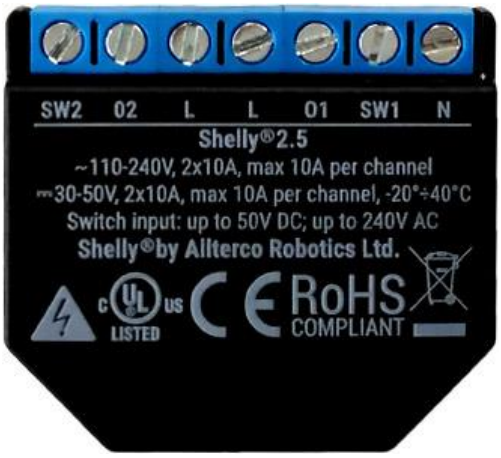
SW2 02 L L 01 SW1 N
Shelly®2.5
~110-240V, 2x10A, max 10A per channel
⎓30-50V, 2x10A, max 10A per channel, -20°÷40°C
Switch input: up to 50V DC; up to 240V AC
Shelly®by Allterco Robotics Ltd.
c UL us
LISTED
RoHS
COMPLIANT

Figure 5: Shelly 2.5

Shelly Dimmer
Figure 6 shows the Shelly Dimmer Wi-Fi actuator. It provides two input channels and one output channel. It can be used to control dimmable lights and monitor their energy consumption. Also, it can detect changes in the state of buttons/contacts to which its input channels are attached.

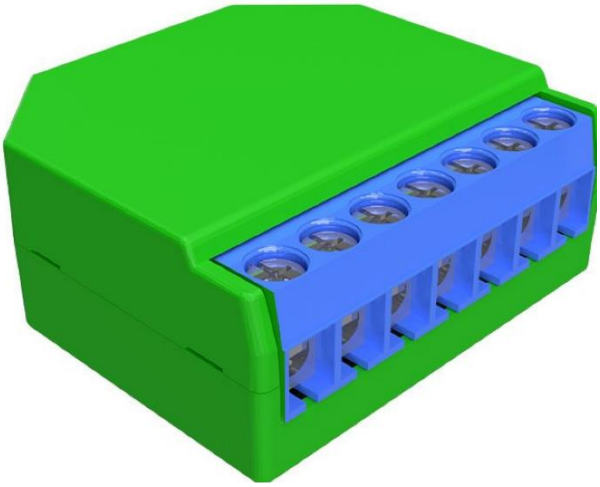

Figure 6: Shelly Dimmer

Shelly RGBW

Figure 7 shows the Shelly RGBW Wi-Fi actuator. It provides one input channel and a number of output channels that can be used to control RGBW led lights. Also, it can detect changes in the state of buttons/contacts to which its input channel is attached to.

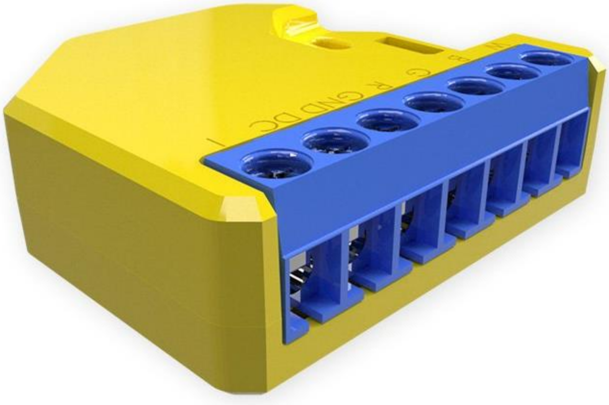

Figure 7: Shelly RGBW

Shelly EM

Figure 8 shows the Shelly EM Wi-Fi actuator. It is a device that can provide the total power and energy consumption of the house where it is installed.

~110-240V, 2 channel energy meter
Shelly® EM
Relay output: ~110-240V, max 2A
www.shelly.cloud
RoHS COMPLIANT
CE
N
0
L
P2-
P2+
P1-
P1+

Figure 8: Shelly EM

2.2.2 Riots Mama

Riots Mama [MAMA] is the gateway of the Riots smart building solution. It connects to the Internet and to the local network using an Ethernet connection. Its role is to collect information sent from the Riots sensor devices (e.g. Riots Thermostats) that use a proprietary wireless protocol.
Riots is currently implementing a WebThings [WoT] compliant firmware for the Riots Mama devices through which all the data gathered from the Riots devices connected to the Mama device can be made available to possible external applications.

Riots Mama	**Information**
Dimensions (width x height x depth)	71mm x 27mm x 71mm
Wireless range	about 10m (*)
Electricity consumption	<0.85 W
Connection	LAN
Operating temperature	+5 - +30°C

Table 1. Riots Mama

Requirements

- Riots Mama requires a power socket

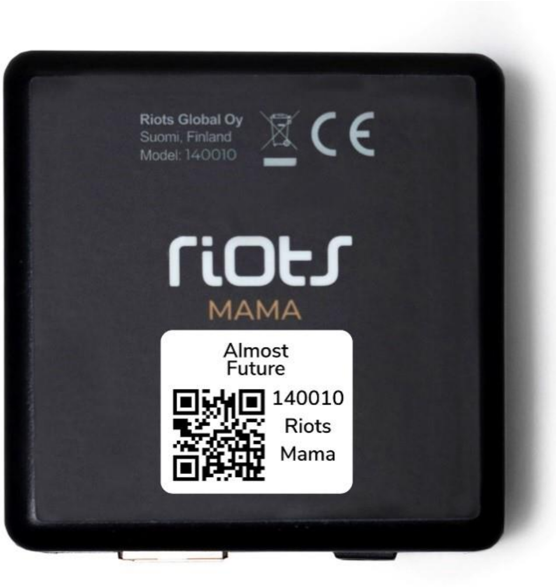

Figure 9: Riots Mama

2.2.3 *Riots Thermostat*

Riots Thermostats [THERMOSTAT] are connected to Riots Mama gateways using a proprietary wireless technology. They are equipped with temperature and humidity sensors and allow setting the desired temperature for the room where they are placed in. The information provided by the Riots Thermostat is going to be offered to the SIFIS-Home framework through the WebThings API provided by the Riots Mama device.

Riots Thermostat	**Information**
Dimensions (width x height x depth)	84mm x 84mm x 21mm
Wireless range	about 10m (*)
Temperature tolerance	± 0,2°C
Humidity tolerance	± 2% RH
Operating temperature	+5 - +30°C

Table 2. Riots Thermostat

Figure 10: Riots Thermostat

3 Final set of Smart Home Use Cases

According to the strategy defined for the overall validation, the pilot will be used to validate the functional requirements of the SIFIS-Home framework. To this end here we report and refine the final list of use cases for the SIFIS-Home project, that is composed of both the use cases defined in D1.2 and the pilot specific use cases reported in D6.1. When a pilot specific use case implements and demonstrates a use case defined in D1.2 we only report the D6.1 use case and highlight the D1.2 use case that it refines.

UC 01 - Login through biometrics
Defined in D1.2

UC 02 - Operate through voice commands
Defined in D1.2

UC 03 - Being alerted if motion sensors detect people presence (covers and implements Get notification about physical intrusion)
Defined in D1.2

UC 04 - Get notification about software intrusion
Defined in D1.2

UC 05 - Register Device
Defined in D1.2

UC 06 - Unregister Device
Defined in D1.2

UC 07 - Configure Device
Defined in D1.2

UC 08 - Install third party applications
Defined in D1.2

UC 09 - Parental control (covers and implements Configure policies to restrict/handle access to functionalities)
Defined in D1.2

UC 10 - Configure user settings
Defined in D1.2

UC 11 - Control statistics and analytics
Defined in D1.2

UC 12 - Remote configuration of device
Defined in D1.2

UC 13 - Remote configuration of policies
Defined in D1.2

UC 14 - Remote handling of emergency situations
Defined in D1.2

UC 15 - Turn on/off lights using the control panel

Use Case #	SIFIS-PI-UC-15
Goal in Context	Allow a user of the smart home to control the devices present in its house by means of a web control panel or a mobile application.
Scope & Level	User goal
Preconditions	The user should be logged in into the system. The devices to control should be active and operational. At least one Smart Device (SD) should be active. If the operation is performed from a remote side, the House should have an active Internet connection.
Success End Conditions	The framework provides a GUI through which it is possible for the smart home user to control its devices (e.g. turn on/off a certain light). When the user requests the execution of a command, the recipient device should change its state.
Failed End Condition	The user is not able to control its devices by using the provided control panel, e.g. he/she is not able to turn on/off a certain light
Primary, Secondary Actors	Resident User, Administrator
Trigger	User opening the device control panel on the mobile application or the web control panel.
Description	1. The Resident user opens the panel that allows controlling the devices present in its house.
	2. The System provides the user with the list of the devices that are inside its house. The GUI should also report the current state of the devices.
	3. The Resident selects a specific device to control.
	4. The System shows a GUI reporting possible commands for the device.

	5. The Resident requests the execution of a certain command.
	6. The command is executed successfully, and the device changes its state. The updated state is reported by the GUI.
Extensions	1a. Due to network errors is not possible to retrieve the list of the devices that are inside the house. The Resident user should be informed about the network error.
	6a. The operation fails. The GUI is not updated and the Resident is informed that the operation was not successfully performed.

UC 16 - Turn on/off lights pressing and releasing buttons

Use Case #	SIFIS-PI-UC-16
Goal in Context	Allow a user of the smart home to turn on/off lights using physical buttons.
Scope & Level	User goal
Preconditions	The devices to control should be active and operational. At least one Smart Device (SD) should be active.
Success End Conditions	The framework recognizes that a physical button has been pressed and then, turns on/off the light connected to the physical button.
Failed End Condition	The light does not turn on/off after pressing its associated physical button.
Primary, Secondary Actors	Resident User
Trigger	The User presses a physical button.
Description	1. The Resident user presses a physical button.
	2. The System detects that a physical button has been pressed.
	3. The System automatically turns on/off the light connected to the pressed button according to the current state of the light.
Extensions	2a. The System does not detect the physical button press event and, hence, the light is not turned on/off.

UC 17 - Being able to interact with the devices only if authorized

Use Case #	SIFIS-PI-UC-17
Goal in Context	Only authorized users should be able to control the physical devices present in the smart home.
Scope & Level	User goal
Preconditions	The devices to control should be active and operational. At least one Smart Device (SD) should be active. At least one NSSD should be active.
Success End Conditions	The framework does not allow unauthorized users to access the smart home functionalities (e.g. control physical devices).
Failed End Condition	It is possible for an unauthorized user to control the physical devices of the smart home.
Primary, Secondary Actors	Resident User
Trigger	The User opens the mobile application or the web-based control panel and provides its credentials.
Description	1. The Resident user opens the mobile application or the web-based control panel and provides its credentials.

	2. The System rejects the login request of the user if he/she is not an authorized user of the smart home.
	3. Authorized Users are provided with a GUI that allows controlling the physical devices of the house.
Extensions	-

UC 18 - Being able to control the house in case of failures

Use Case #	SIFIS-PI-UC-18
Goal in Context	The User of the smart home should be able to control its physical devices if a partial system failure occurs
Scope & Level	User goal
Preconditions	The devices to control should be active and operational. At least two Smart Devices (SD) should be active.
Success End Conditions	The System allows the user to control its physical devices in case of a partial system failure.
Failed End Condition	The User is not able to control its devices in case a partial system failure occurs.
Primary, Secondary Actors	Resident User
Trigger	One Smart Device experiences a failure and becomes inactive. The User wants to control its physical devices after the failure of the Smart Device occurred.
Description	1. The User uses the web-based control panel or the mobile application to send a device command.
	2. The System executes the command correctly and the state of the device changes.
Extensions	2a. The System is not able to execute the command due to the partial system failure.

UC 19 - Being alerted if a device is generating anomalous traffic

Use Case #	SIFIS-PI-UC-19
Goal in Context	The User of the smart home should be alerted if a device generates anomalous traffic (e.g. the network traffic generated by the device increases significantly).
Scope & Level	Emergency management.
Preconditions	At least one Smart Device (SD) should be active. At least one NSSD is active.
Success End Conditions	The framework detects that a device is generating anomalous traffic and sends a notification to the user.
Failed End Condition	- The framework does not detect that a device is generating anomalous traffic. - The framework detects the anomalous traffic conditions, but the user is not notified.
Primary, Secondary Actors	Resident User
Trigger	A NSSD starts generating anomalous traffic
Description	1. The System detects the anomalous traffic conditions

	2. The User is alerted of the event (a notification is reported in the notification panel of the mobile application or in the web-based control panel)
Extensions	-

4 Acceptance tests for the use cases

In the present section the acceptance, system level, testing procedure for the pilot use cases is described.

4.1 *Functional validation*

In this section, we describe the validation procedure for the functional requirements of the SIFIS-Home framework. The validation is based on the execution of End-to-End (E2E) test cases. A specific test case has been defined for each of the use cases in the final set reported in section 3 of the present deliverable.

All test cases were designed as manual test cases following the steps of the use cases. The test cases results will be logged in a systematic way [TESTLOG].

Table 3 reports the adopted test strategy: for each use case, the way the use case will be implemented, and the testing technique that will be adopted.

Use Case	Implementation in the pilot	E2E Test technique
UC 01 - Login through biometrics	For the pilot implementation of this use case, we are going to use a Laptop (SD) provided with a camera. The identity of the user will be recognized through a Face Recognition operation.	A Resident User for which a face model has been registered into the System will enter inside a certain room. If the Resident is identified by the System, a notification of successful recognition of the User will be sent. Otherwise, a notification event reporting a failure in identifying the User will be generated. The test will be repeated with multiple different Resident users.
UC 02 - Operate through voice commands	For the pilot implementation of this use case, we are going to use a Laptop (SD) provided with a microphone, or a smartphone. Also, the DoMO Wi-Fi actuators and physical lights will be used Then, voice commands will be sent to the System.	A Resident User will issue a specific voice command (e.g. “turn on the light”). If the command is successfully recognized by the System a light will be turned on. Otherwise, a notification will be sent reporting that the command was not intelligible. The test will be repeated with multiple different Resident users.
UC 03 - Being alerted if motion sensors detect people presence	For the pilot implementation of this use case, we are going to use a DoMO gateway and a Wi-Fi actuator to which a motion sensor is connected to.	A person will enter inside a certain room and motion will be detected. The motion event should be reported in the Notification panel of the mobile application and the web control panel.

UC 04 – Get notification about software intrusion	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	We are going to install and execute a malware on the DoMO gateway. The software intrusion should be detected and reported to the user through Mobile application notification panel.
UC 05 – Register device	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator.	An authorized User will open the mobile application and use a specific control panel to register a DoMO Wi-Fi actuator (NSSD) into the system. The mobile application should ask the user to provide the details of the NSSD to be inserted into the system (e.g. MAC address, user/password pair to use to communicate with the device). After the device is inserted into the system, it should be possible to control it from the control panel.
UC 06 – Unregister device	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator.	An authorized User will open the mobile application and use a specific control panel to un-register the DoMO Wi-Fi actuator (NSSD). After the device is unregistered is should not be reported anymore in the device list. Also, it should not be possible to control it.
UC 07 – Configure device	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator.	An authorized User will open the mobile application and use a specific control panel to configure a specific DoMO Wi-Fi actuator (NSSD). From the panel it should be possible to change the device configuration, e.g. specify the specific physical objects (lights, sockets, etc) to which the actuator is connected to.
UC 08 – Install third party applications	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	An authorized User will open the mobile application and use a specific control panel to obtain the list of the third-party applications that can be potentially installed into the System. The user will select a specific third party application for installation. At the end of the procedure, the application should be installed on the Smart Device.
UC 09 – Parental control	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	The User will open the mobile application. The System should allow the User to define new policies or change existing ones. In detail, we are going to define a policy that does not

		allow turning on the appliances of a certain room when there are children inside.
UC 10 – Configure User Settings	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	The Administrator User will open the mobile application and use the User control panel. The User control panel should allow the Administrator to define policies for the different users.
UC 11 – Control statistics and analytics	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	The User will open the mobile application and will select a specific device. The mobile application should report a log and an information panel that reports the main events related to the device.
UC 12 – Remote configuration of device	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	The User will open the mobile application when he/she is on a remote side. The System should allow the User to change the configuration of a device.
UC 13 – Remote configuration of policies	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	The User will open the mobile application when he/she is on a remote side. The System should allow the User to define new policies or edit existing ones.
UC 14 - Remote handling of emergency situations	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator connected to an alarm contact sensor.	We open the alarm contact sensor. The event should be reported in the Notification panel of the mobile application and on the web-based control panel. The User should be provided with system logs and should have the possibility to control the house to, for example, turn off the alarm.
UC 15 – Turn on/off lights using the control panel	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator connected to a physical Light.	The User will open the mobile application and will use the control panel to get the list of the devices that are installed inside his/her house. The mobile application should show the possible commands for the different devices. The User will then use the GUI controls to turn on a certain Light. The Light should be turned on and the new Light state should be updated on the UI.
UC 16 – Turn on/off lights pressing/releasing buttons	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a DoMO Wi-Fi actuator connected to both a physical Light and a physical button.	The User will press the physical button. The System should detect the button press event and turn on/off the Light.

UC 17 – Being able to interact with the devices only if authorized	For the pilot implementation of this use case, we are going to use a DoMO gateway and a smartphone.	An Authorized User will perform a login operation. The operation should succeed. An Unauthorized User will perform a login operation. The operation should fail.
UC 18 – Being able to control the house in case of failures	For the pilot implementation of this use case, we are going to use 2 DoMO gateways, a smartphone and a DoMO Wi-Fi actuator connected to a physical light.	We start the test with the 2 DoMO gateways active and operational. We verify that it is possible to turn on/off the physical light. We turn off the DoMO gateway to which the DoMO Wi-Fi actuator is connected to. After some time from the deactivation of the DoMO gateway, we issue the turn on/off command again. It should still be possible to control the physical light.
UC 19 – Being alerted if a device is generating anomalous traffic	For the pilot implementation of this use case, we are going to use a DoMO gateway, a smartphone and a NSSD.	We simulate an anomalous traffic condition by changing the program/firmware executed by the NSSD. The System should detect the anomalous traffic condition and report the event in the Notification panel of the mobile application.

Table 3. Pilot implementation and E2E test case for every use case

Here, we also report the updated list of the functional requirements. For every requirement we specify the updated list of affected use cases.

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, UC17	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 administrators the facility to control their home appliances through their speech.	UC2	C	PE-02 PE-06 DE-02 DE-03	Performance Performance 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, UC14	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, UC19	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, UC19	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, UC19	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, UC19	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, UC15, UC18	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		

To evaluate the results of the validation phase once the tests are performed against the pilot implementation, we adopt the GQM template by Basili et al [GQM], to define a set of measurements for the testing results.

The used GQM template is reported in the following table.

Object of study	SIFIS-Home framework
Purpose	Validation of the main use cases
Focus	Functional requirements
Perspective	End user (E2E testing)
Context	Pilot implementation

The GQM questions and metrics for every E2E test case are reported below.

Use Case	GQM questions	GQM metrics
UC 01 - Login through biometrics	Q1.1: Is a Resident User recognized by the System? Q1.2: Is a Non-Resident User not recognized by the System? Q1.3: Is a notification sent when the Resident is recognized? Q1.4: Is a notification sent when the Non-Resident is not recognized?	M1.1: Percentage of resident users that are correctly recognized by the system. M1.2: Percentage of non-resident users that are recognized as resident users by the system. M1.3: Percentage of notifications correctly sent upon resident notification. M1.4: Percentage of notifications correctly sent upon non-resident notifications.
UC 02 - Operate through voice commands	Q2.1: Is the voice command executed successfully by the System? Q2.2: Is a notification generated if the voice command is not intelligible?	M2.1: Percentage of voice commands that are correctly executed by the system. M2.2: Percentage of notifications correctly generated upon not intelligible voice commands.
UC 03 - Being alerted if motion sensors detect people presence	Q3.1: Is the people presence detected by the System? Q3.2: Is the motion event reported by the System?	M3.1: Percentage of motion events that have been successfully reported during testing. M3.2: Number of false motion events that have been reported during testing.
UC 04 – Get notification	Q4.1: Is the malware execution detected? Q4.2: Is the software intrusion reported to	M4.1: Number of times the software intrusion event has been

about software intrusion	the user?	successfully detected. M4.2: Percentage of false software intrusions that have been detected.
UC 05 – Register device	Q5.1: Is the device correctly registered into the system? Q5.2: Is it possible to control the device after it has been registered into the system?	M5.1: Percentage of devices that are correctly registered after a testing session. M5.2: Percentage of controllable devices of those registered.
UC 06 – Unregister device	Q6.1: Is the device correctly unregistered from the System? Q6.2: Is it possible to control the device after it has been deregistered?	M6.1: Percentage of correctly unregistered devices after a testing session. M6.2: Percentage of controllable devices of those that are deregistered.
UC 07 – Configure device	Q7.1: Is the current configuration of the device available to the smart home users? Q7.2: Is it possible to change the configuration of the device?	M7.1: Percentage of users to which the current configuration is available. M7.2: Percentage of users that are able to change the configuration of the device.
UC 08 – Install third party applications	Q8.1: Is it possible to get the list of 3rd party applications? Q8.2: Is the installation of a 3rd party application performed successfully?	M8.1: number of 3rd party applications retrieved. M8.2: percentage of 3rd party applications that are correctly installed.
UC 09 – Parental control	Q9.1: Is it possible to create the policy required for parental control?	M9.1: existence of a policy for parental control.
UC 10 – Configure User Settings	Q10.1: Is it possible to retrieve the list of the configured users? Q10.2: Is it possible to define different policies for the different users?	M10.1: number of configured users. M10.2: number of policies for the users.
UC 11 – Control statistics and analytics	Q11.1: Are statistics and analytics reported for every device?	M11.1: percentage of devices for which statistics and analytics are correctly reported.
UC 12 – Remote configuration of device	Q12.1: Is it possible to configure a device from a remote side?	M12.1: percentage of devices that can be configured from remote.
UC 13 – Remote configuration of policies	Q13.1: Is it possible to configure and edit policies from a remote side?	M13.1: percentage of policies that can be configured from remote.
UC 14 - Remote handling of emergency situations	Q14.1: Is the emergency reported in the Notification panel of the mobile application? Q14.2: Is it possible for the users to interact with the House after the emergency notification is received?	M14.1: Number of times a false contact sensor activation is reported. M14.2: Percentage of contact sensor activations that have been successfully reported.
UC 15 – Turn	Q15.1: Is it possible to get the list of	M15.1: number of installed

on/off lights using the control panel	installed devices? Q15.2: Is it possible to get the list of commands for a certain device? Q15.3: Are commands executed successfully?	devices retrieved. M15.2: number of commands retrieved for each device. M15.3: percentage of commands executed successfully.
UC 16 – Turn on/off lights pressing/releasing buttons	Q16.1: Is the button press event detected and reported? Q16.2: Is the light turned on/off after a button press event?	M16.1: Number of times the system failed in detecting a button press event. M16.2: Percentage of successful detections of button press events.
UC 17 – Being able to interact with the devices only if authorized	Q17.1: Is an Authorized User able to perform a login operation? Q17.2: Is the login request of an Unauthorized user rejected?	M17.1: Percentage of successful logins by authorized users. M17.2: Percentage of successful logins by unauthorized users.
UC 18 – Being able to control the house in case of failures	Q18.1: Is it possible to control the devices of the house before the Smart Device failure occurs? Q18.2: Is it possible to control the devices of the house after the Smart Device failure?	M18.1: number of devices that can be controlled before the smart device failure occurs. M18.2: number of devices that can be controlled after the smart device failure occurs.
UC 19 – Being alerted if a device is generating anomalous traffic	Q19.1: Is the anomalous traffic condition detected? Q19.2: Is the user informed that a device is generating anomalous traffic?	M19.1: Number of times the anomalous traffic event has been successfully detected. M19.2: Percentage of false anomalous traffic events that have been detected.

Table 4: GQM questions

For the purpose of evaluating the overall outcome of testing purposes for functional requirements, we also consider two additional aggregate metrics, described below:

1) **N_uc**: Number of use cases that the pilot is able to demonstrate. Such metric is computed as the raw count of the use cases for which a test case is run successfully;
2) **N_fr**: Number of functional requirements that are covered by the pilot. Such metric is computed as the sum of the functional requirements that are covered by the use cases that were successfully run in the acceptance testing phase.

5 Conclusion

This deliverable provides the updated list of devices that we plan to use for the final SIFIS-Home pilot implementation. Moreover, all the different smart home use cases that are going to be implemented, validated and tested using the pilot implementation are presented in detail. Also, End-to-End (E2E) acceptance test and GQM questions for every use case are reported and discussed.

6 References

[GQM] Basili, Victor R. *Software modeling and measurement: the Goal/Question/Metric paradigm*. 1992.

[TESTLOG] Din, George, Justyna Zander, and Stephan Pietsch. *Test execution logging and visualisation techniques*. 17th International Conference Software and Systems Engineering and their Applications, Paris, France. 2004.

[BANANA PI] Banana Pi open source hardware community, https://www.banana-pi.org/

[RASPBERRY PI] Computing for everybody, https://www.raspberrypi.com/

[SHELLY] Easy Smart Home Automation, https://www.shelly.cloud/en

[MAMA] Riots Mama https://riots.fi/en/tuotteet/mama

[THERMOSTAT] Riots Thermostat https://riots.fi/en/tuotteet/huonetermostaatti

[WoT] Web Of Things (WoT) Architecture, https://www.w3.org/TR/wot-architecture/

Glossary

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