SCOTT:

Secure COnnected Trustable Things

Applicability of Use Case and Building Blocks for Assisted Living Demonstrated (Iteration 3)

Document Type	Deliverable
Document Number	D21.6
Primary Author(s)	Frank van de Laar | PRE (Editor)
Document Version / Status	1.0 | Final
Distribution Level	PU (public)

Project Acronym	SCOTT
Project Title	Secure Connected Trustable Things
Project Website	www.scottproject.eu
Project Coordinator	Michael Karner | VIF | michael.karner@v2c2.at
JU Grant Agreement Number	737422
Date of latest version of Annex I against which the assessment will be made	2019-03-15

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

CONTRIBUTORS

Name	Organization	Name	Organization
Frank van de Laar	PRE	Mateusz Mul	GUT/Vemco
Raja Ramachandran	PRE	Patryk Kaczmarek	Vemco
Francesco Pessolano	Xetal	Hamed Arshad	UiO
Aaqib Saeed	TU/e	Christian Johansen	UiO
Lars Thomas Boye	Tellu	Lukasz Szczygielski	GUT
Niels Jacot	Wolffia		

FORMAL REVIEWERS

Name	Organization	Date
Ramiro Robles	ISEP	2020-02-13
Peter Moertl	VIF	2020-02-10

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.1	2020-01-07	Frank van de Laar / PRE	First skeleton draft by partially filling in some of the Sections and creating placeholders for other contributors.
0.2	2020-01-21	Frank van de Laar / PRE	Inserted TU/e, Vemco, Xetal and Wolffia contributions
0.3	2020-01-24	Frank van de Laar / PRE	Inserted PRE contribution
0.4	2020-02-03	Frank van de Laar / PRE	Inserted GUT contributions (incl. section 4).
0.5	2020-02-04	Frank van de Laar / PRE	Inserted UiO contribution
0.6	2020-02-06	Frank van de Laar / PRE	Added Conclusions, updated 3.3.2
0.7	2020-02-07	Frank van de Laar / PRE	Version for Review, various updates
0.8	2020-02-18	Frank van de Laar / PRE	Updated, based on reviewers' comments
1.0	2020-02-21	Frank van de Laar / PRE	Final version, all changes accepted

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 7

2 OBJECTIVES 8

2.1 Use Cases 8

3 ASSISTED LIVING AND COMMUNITY CARE USE CASE 9

3.1 Context of the Use Case 9
3.2 High Level Architecture of the Use Case Components 9

3.2.1 SCOTT reference architecture 10
3.2.2 Security scan 11
3.2.3 Privacy labelling 11

3.3 Achievements 11

3.3.1 TU/e 12
3.3.2 PRE 13
3.3.3 Vemco 20
3.3.4 GUT 22
3.3.5 Xetal 24
3.3.6 UiO 27
3.3.7 Tellu 28
3.3.8 Telenor, OsloMet and Wolffia 31

4 EMERGENCY DEPARTMENT EQUIPMENT AND PATIENT TRACKING USE CASE 34

4.1 Context of the use-case 34
4.2 High level architecture of the Use Case components 34
4.3 Achievements 35

5 DISSEMINATION, EXPLOITATION AND STANDARDISATION 38

5.1 Exploitation 38
5.2 Dissemination 38
5.3 Standardization 39

6 INTEROPERABILITY 40

7 LINK TO TECHNOLOGY LINES 41

8 CONCLUSIONS 42

9 REFERENCES 43

A. ABBREVIATIONS AND DEFINITIONS 44

LIST OF FIGURES

Figure 1: Use case architecture of the ALCCS with mapping to SCOTT Technical Building Blocks (BB). 10
Figure 2: Updated Layered entity model. 11
Figure 3: Overview of the logical layers in federated learning system. 12
Figure 4: Unsupervised representation learning in federated context. 13
Figure 5: Connectivity chain for LoRa elderly UI using OTAA in the ALCCS demonstrator. 14
Figure 6: Screenshot of capturing device id with an open source Android application. 15
Figure 7: Connectivity setup of NB-IoT or LTE-M based IoT device with eSIM. 17
Figure 8: Office room for setup of empirical evaluation 19
Figure 9: System architecture of DecaWave and on-body testing of DecaWave tags 19
Figure 10: Adding an elderly's home in the app. 21
Figure 11: Adding a caregiver 21
Figure 12: Showing a caregiver with an activated mobile access card 22
Figure 13: CI/CD pipelines - MPS 23
Figure 14: MPS entity in TU/s building in Eindhoven - UI screenshot. 23
Figure 15: First Xetal Yugen sensor prototypes differing in area coverage, processing power and acquisition speed. 24
Figure 16: Latest Xetal Yugen prototype (40x120 FoV) inclusing a wireless module connected to its back. 25
Figure 17: Xetal Yugen Hub used to aggregate data from several sensors and upload it to the Yugen Fusion Server. 25
Figure 18: Example of installation for development and testing of multiple Xetal Yugen sensors connected in a network. 26
Figure 19: Example where the data from a network of 6 Yugen sensors is used for monitoring an office floor. 26
Figure 20: Example data the server provides out of several Yugen sensors in a building in order to provide information about flow and presence of people in a given area. 26
Figure 21: Example of thermal map provides by the server for a sensor used to monitor a meeting area. 27
Figure 22: The overall schema of applying SABAC in WP21 28
Figure 23: Dexcom patch with sensor (top left) and applicator. 29
Figure 24: Screenshots from the Tellu Medical Gateway app. 30
Figure 25: TelluCloud ID authentication in browser. 31
Figure 26 Network slices 32
Figure 27: Emergency Department Equipment and Patient Tracking Use Case – Overview. 34
Figure 28: HLA - Physical entity model 35
Figure 29: Adding a new location in the MPS UI 36

Figure 30: Device provisioning overview 36
Figure 31: The Head of the hospital presenting a plan of the building. 38

LIST OF TABLES

Table 1: Localization Requirements, specifications and evaluation. 18

1 EXECUTIVE SUMMARY

This document describes what is achieved in the third iteration of WP21 with reference to the scenarios specified in D21.5 [1]. In order to make this document better readable for a wider public, the use case descriptions and architecture diagrams have been copied from previous documents in the introduction of sections 2 and 3.

The Assisted Living and Community Care System (ALCCS) use case description at the start of the second iteration (D21.3 [3]) has been refined with new insights obtained during the implementation phase of that iteration (D21.4 [4]) mainly in order to improve robustness and user friendliness. The 2nd use case for Emergency department, equipment and patient tracking has been worked out in further detail and includes preparations for a pilot in the Emergency Department of a hospital.

Generally speaking, the focus in this 3rd iteration of WP21 has been on investigating for further deployment of the scenarios, techniques and devices as applied in the use-case demonstrator(s). Furthermore, this 3rd iteration aimed to gain more in-depth technology insights (e.g. network slicing, LPWAN, Real Time Locating Systems, Multimodal Positioning Systems), and generally knowledge that can be disseminated in follow-up projects and products.

Keywords: healthcare, elderly care, IoT, IoMT, context derivation, access control, Direct-to-Cloud, LPWAN, 5G, LoRa, NB-IoT, Cat-M1, localization, RTLS, MPS, FHIR, diabetes monitoring, ambulatory patient monitoring, SABAC, network slicing, sensor fusion.

2 OBJECTIVES

The objectives of the deliverable, the work package, and the link to the overall SCOTT objectives have been stated in D21.1 [3]. A total of three iterations were planned throughout the course of SCOTT to reach these objectives. The main objectives have been achieved as indicated below:

- Provide a solution for secure **trust-based delegation** in assisted living and community care. This has been solved using an architectural model in which elderly or patient data is kept on premise and separated from caregiver data in the cloud. Only in case when really needed (for example an emergency event) the required data is provided to selected caregiver(s). A novel aspect of this solution is that the most appropriate Caregiver is selected based on the actual context of the resident, whereas present-day solutions patch the resident through to a centralized call center.
- Provide solution for automated **context derivation for resident as well as potential responders**. This was achieved a.o. by the combined use of various wirelessly connected sensors monitoring the resident's home, as well as his/her vital signs to assess personal health, wellbeing (specifically fall detection) and supporting geolocation and attribute based access control to select the most appropriate responder. In the 3rd iteration these topics have been investigated for further improvements.
- **Realize a demonstrator** integrating the abovementioned trust-based delegation and automated context derivation functionalities, which showcases the combined functionality supporting the use case and therefore enabling validation of the concept from an end-user perspective. This demonstrator was already made in the 1st iteration, improved and extended upon in the 2nd iteration and further investigated for wider deployment in the 3rd iteration.

2.1 Use Cases

As discussed in D21.5 [1] for this third iteration, two different use cases have been identified – Assisted Living and Community Care (ALCSS) and Emergency Department Equipment and Patient Tracking – which are described successively in Sections 3 and 4.

Specific technical requirements such as sensor data rates, sampling frequencies, latency, and reliability have not been listed for the ALCCS as they may differ for specific applications and sensor types. For example, the requirements for Emergency Department Equipment and Patient Tracking have been identified as listed in Table 1.

3 ASSISTED LIVING AND COMMUNITY CARE USE CASE

This section describes the main body of work achieved by WP21 during the third iteration on the ALCCS. In Section 3.1, a brief recap of the context and purpose of the ALCCS is given. Subsequently, Section 3.2 updates the system architecture description from D21.5 [1]. Finally, in Section 3.3, the actual achievements to date of WP21 partners are detailed out.

3.1 Context of the Use Case

This use case is about an integrated ALCCS for elderly monitoring and caregiver notification in case of emergency events. The primary goal of this system is to do reliable fall detection and sent an alarm event to available caregiver(s) when needed. A selected caregiver is then temporarily granted access to the elderly home for help. This demonstrator also supports a glucose monitoring system for diabetes patients as described in D21.3 [5]. Optionally the system may be extended with other healthcare related monitoring functions (for example vital signs). This integrated ALCCS demonstrator was build and tested by various partners as listed in 3.3 in the 1st and 2nd iteration of this WP. A 5G network slicing based solution for the ALCSS has also been investigated. Careful considerations have been made with respect to architecture, technologies and standards to provide a demonstrator that is expected to be secure, trustable, and expandable.

3.2 High Level Architecture of the Use Case Components

The final ALCCS architecture is shown below for reference. The elderly UI device is a wearable device that performs fall detection using an accelerometer. It also has a panic button for urgent help requests. The positioning systems are ceiling mounted devices monitoring presence and fall detection based on positional changes. The monitoring signals are combined in the on-premise Elderly Context Deviation (ECD) that may send an incident event to the caregiver selection logic to involve a caregiver, which is temporarily granted access to the elderly's home with the Physical access Control function.

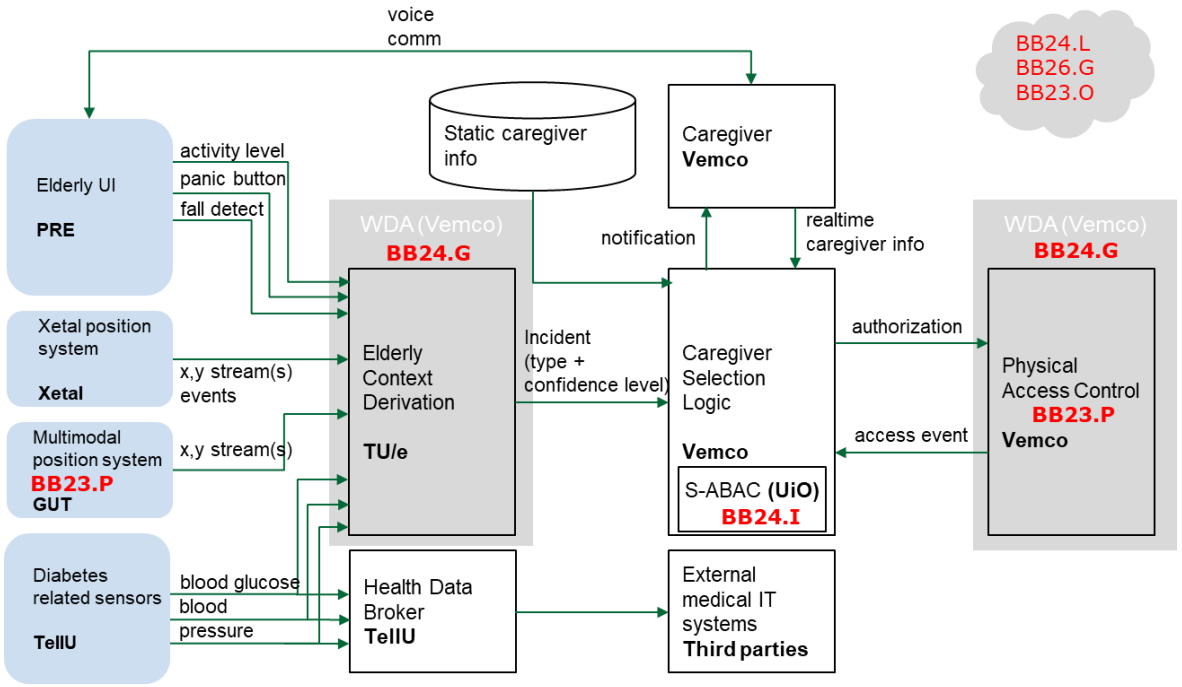

Figure 1: Use case architecture of the ALCCS with mapping to SCOTT Technical Building Blocks (BB).

3.2.1 SCOTT reference architecture

The implementation of the SCOTT reference architecture in ALCCS is presented and described using two different, complementary perspectives – the layered entity model and the physical entity model. There are no changes in the ALCCS physical entity model as shown in D21.5 [1] (section 3.2). The layered entity model of the ALCCS implementation has been updated in correspondence with the latest SCOTT reference architecture [6] as shown below.

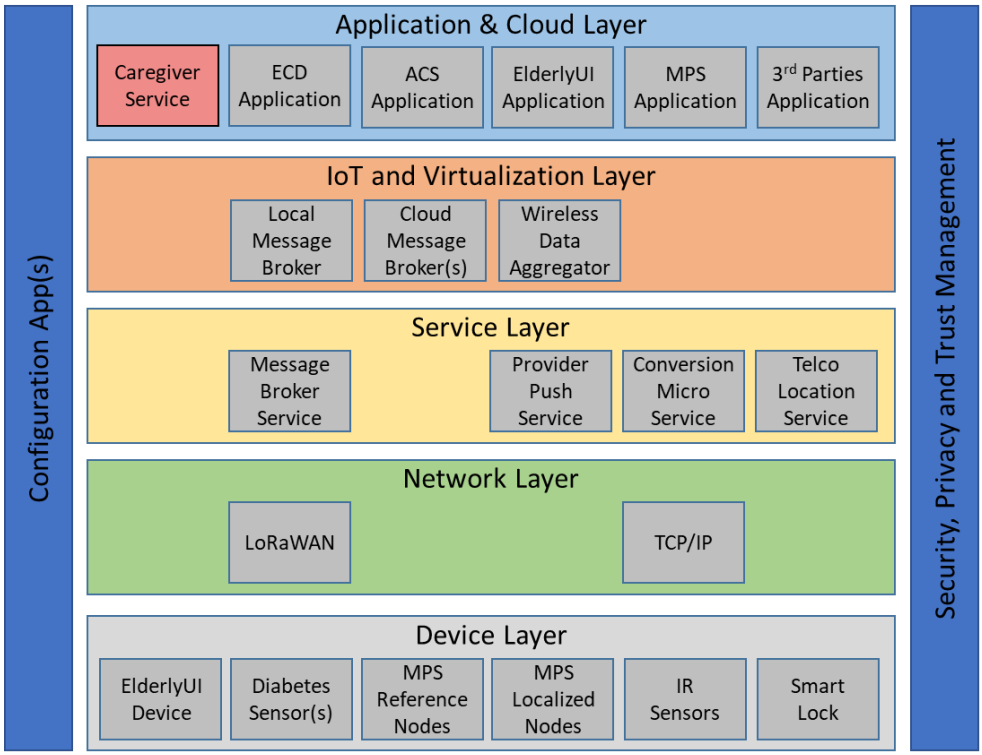

Figure 2: Updated Layered entity model.

3.2.2 Security scan

A step by step Security classification methodology has been prepared by BB26.F by defining the concepts and levels of connectivity, protection, exposure and impact of successful cyber-attack as the components of the security classes [7]. The connectivity levels (C1-C5) have been defined from a completely isolated system to distributed systems with public infrastructure. The protection level (P1-P5) requirements have been also determined based on protection criteria and security functionality. Based on connectivity and protection levels, the level of exposure (E1-E5) is calculated. Then by identifying the level of the impact of successful cyber-attacks and calculated exposure, the security class (A-F) can be achieved.

The ElderlyUI component of Assisted Living and Community Care Architecture (ALCCS) will be analysed according to this method. The results of this analysis result in a security classification (A-F) and also shows which specific security aspects of a device should be improved in order to achieve a better security class.

3.2.3 Privacy labelling

An assessment of the ALCCS use-case has been used as input for a whitepaper on Increase User Trust for a Bigger Market of Digital Technologies [8] from BB.26.G (WP26).

3.3 Achievements

This section zooms in on partners' technical achievements during this third iteration. The following subsections describe the status of the integrated Assisted Living and Community Care System (ALCCS) demonstrator and related future extensions.

3.3.1 TU/e

TU/e dedicated the efforts towards developing a federated learning framework to simulate machine learning on-the-edge. The Internet of things (IoT) devices generate a vast amount of unlabelled data that can be utilized for training machine learning models. Currently, machine learning models are developed with user data that are aggregated in a centralized system. However, current systems cannot keep up with aggregating an ever-increasing amount of data. Besides, storing user data in a central location is raising privacy concerns. Therefore, a privacy-preserving, distributed machine learning technique is known as Federated Learning (FL), is gaining popularity. FL has been used effectively in supervised learning use cases, where labels can be generated implicitly based on user interaction. Annotating the data through explicit user labelling is undesirable in several cases (e.g., sensor analytics), which is required for learning supervised models. The end-users are not motivated to label without provision of adequate rewards, are not available on-demand, and have the potential to introduce faulty labels due to fatigue or malignancy and raise privacy concerns.

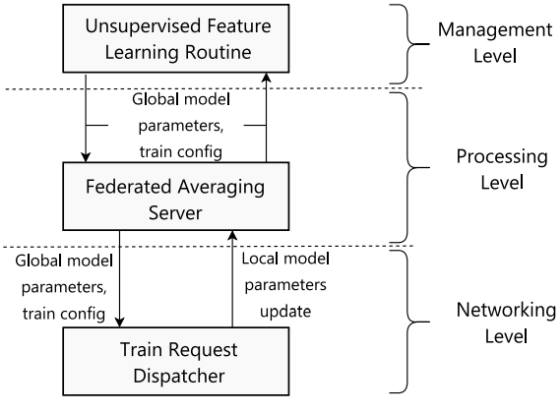

Figure 3: Overview of the logical layers in federated learning system.

An approach for utilizing unlabeled data in FL setting is presented for developing deep learning models through self-supervision [9]. For this purpose, a system was designed that manages training, neural network architecture selection, client availability, and other configuration details for achieving distributed learning. The high-level overview of the system design is illustrated in Figure 2. For learning a model from unlabeled input, auto-encoders and transformation prediction networks are utilized [5]. The features are learned from entirely unlabeled input in a federated setting and used for solving end-task of interest (i.e., activity detection) in a centralized environment. The entire learning flow is provided in Figure 3. This method achieves performance that is close to fully supervised models, i.e., when entire labeled data is available for learning models in an end-to-end manner.

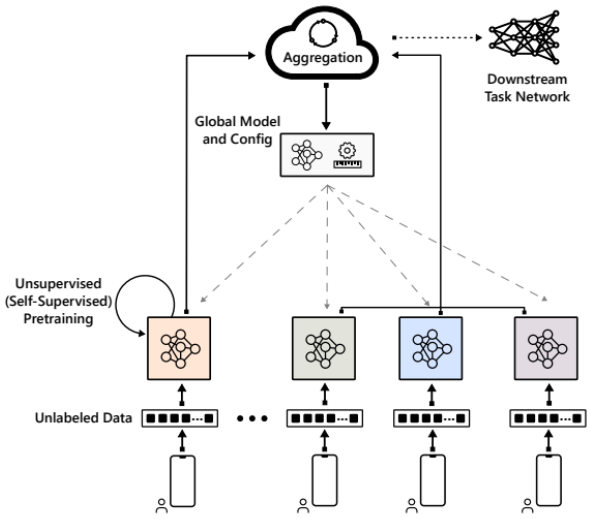

Figure 4: Unsupervised representation learning in federated context.

Furthermore, to improve the Elderly Context Derivation (ECD) system, progress was made towards the integration of GUT's MPS. The GUT fixed the positing system at TU/e, and its integration will be achieved based on the feasibility of the generated data to improve the ALCSS demonstrator in the remaining period.

3.3.2 PRE

For the 3rd iteration PRE explored the following topics w.r.t. to the deployment of the elderlyUI:

1. Easy device to network commissioning to support large-scale deployment of IoT devices
2. HL7/FHIR standard based device registration and observation reporting to support patient monitoring applications.
3. Cellular (NB-IOT and CAT-M1) based connectivity (instead of LoRa) of the ElderlyUI to support global device operation.
4. Real Time Locating System (RTLS) technologies to support (indoor) localization for device (i.e. elderly/patient) tracking in emergency cases.

Each of these explorations is described in more detail in the following subsections.

3.3.2.1 Lora Device Commissioning and Security

The current ElderlyUI in the ALCCS demo network setup is based on LoRa Activation By Provisioning (ABP) which is more simple but possibly less secure because of the use of static keys for data encryption. For large scale deployments it is recommended to use Over The Air Activation (OTAA) because device activation on the network will be confirmed and the session keys will be renewed for each activation. Figure 5 shows how the Elderly UI in the ALCCS demonstrator will be connected to the cloud when using OTAA. The connection consists of 3 stages:

1. A LoRa connection from the IoT device to the network server via one or more LoRa gateways. This connection setup requires an IoT device unique identifier (DevEUI), a network server unique identifier (AppEUI) and an application specific key (AppKey).

2. An internet connection from the LoRA network server to an Amazon Web Service (AWS). This connection setup requires an application Specific Identifier (AS_ID) and an Application Specific Key (ASKEY).
3. An internet connection from AWS to the ECD using a RabbitMQ message broker. This connection setup requires TLS certificate(s) exchange and a user/password authentication.

Using OTAA instead of ABP for the device will not change the 2nd and 3rd connection setup.

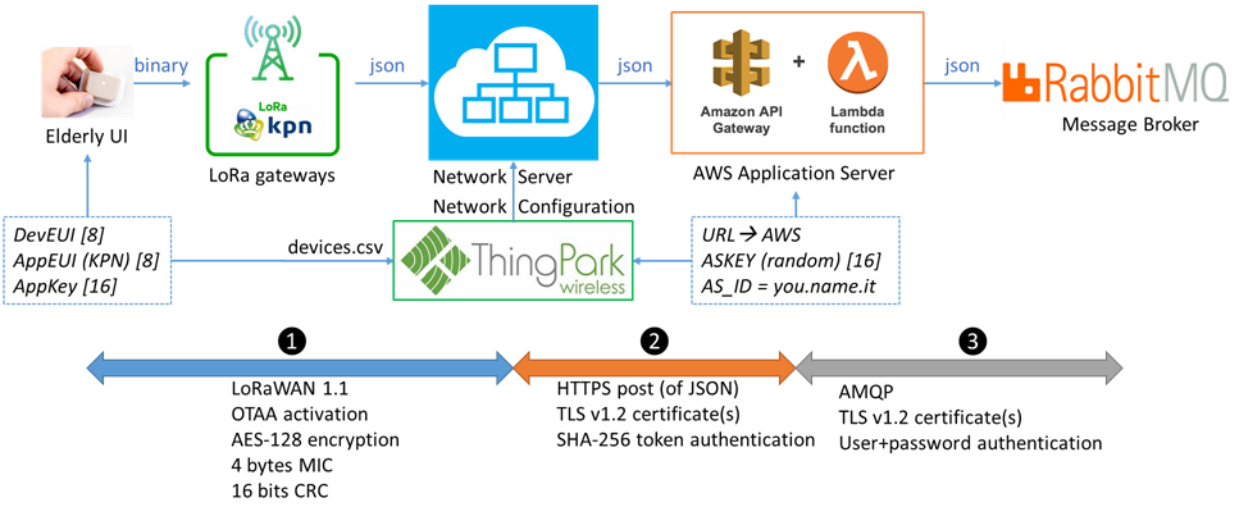

Figure 5: Connectivity chain for LoRa elderly UI using OTAA in the ALCCS demonstrator.

Device key and address management for a large number of devices requires an automated process to prevent manual registration of hundreds or even more security keys (of 16 bytes each) at both the device and network side. This is done following these three configuration steps:

1. Device configuration to provide each device with its own devEUI, Appkey and (common) AppEUI from an automatically generated (CSV) list.
2. Network configuration using the ThingPark network server configuration application [10] to provide the network server with the same (CSV) device list to securely identify registered devices to the network.
3. Network server setup using the ThingPark network server configuration application to provide the AS_KEY (16 bytes), the AS_ID string and the application server URL to the network server.

If the application server considers uplink data messages as authentic (based on AS_ID and a SHA token derived from AS_KEY) it will forward the relevant application data to the RabbitMQ message broker for delivery to the Elderly Context Derivation ECD for further processing.

3.3.2.2 FHIR based device tegistration and patient linking

In addition to connecting the device to the cloud, it is also required to link the device(s) to a patient or care receiver (and possibly also to caregivers) in a private and secure way. In order to achieve this, the elderly and caregiver's data is stored in a separate list or database in the cloud. In the current ALCCS demo this is done by manual system configuration, but this is not a suitable method for larger scale operation.

When the LoRa device is activated on the network the device identity (DevEUI) is associated with an elderly identity.[1] This will typically be done by a caregiver who provides the device to the elderly, by scanning a unique bar code on the elderlyUI device (and not typing in the eight digit DevEUI) and selecting the elderly from a list to whom the elderlyUI device data will be associated with. The result of the selection should be sent back to the cloud. Information that can directly identify the patient or caregiver is not sent along with the device data during monitoring operation.

In order to validate the concept of easy device commissioning on a larger a scale a trial was setup with a next generation wearable LoRa device. The application area for this device may either be elderly monitoring (elderlyUI) or patient monitoring in general (IoMT device).

3.3.2.2.1 Device commissioning

A mobile application is used for the setup for manual coupling of the device id, the caretaker id and the caregiver id. No personal information is transmitted, but only id's that can be linked to personal data securely stored at the backend. The process of identification has been simplified by using scan codes with a scanning function as shown in Figure 6.

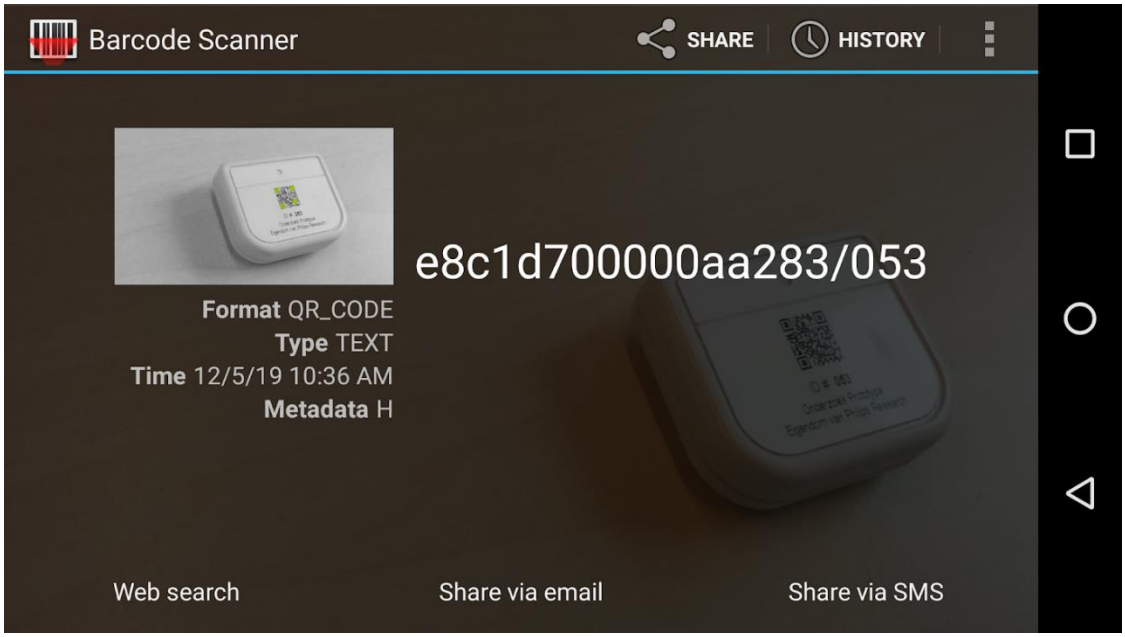

Figure 6: Screenshot of capturing device id with an open source Android application.

3.3.2.2.2 Using FHIR resources

In a healthcare context device, patient and practitioner information may be handled in a standardized way as resources in a FHIR based infrastructure [11]. Measurements results from the device will be stored as observation resources in a FHIR server database along with other related resources [12]. Transaction of resources using HTTP request/response with JSON (or XML) formatted data can be done using interactions as defined by the FHIR RESTful API. This API is already supported by a.o Microsoft Azure and Google's cloud Healthcare API (but not by AWS). Support from these major IoT platforms further enables large scale deployment and interoperability of a FHIR based IoT healthcare concept.

[1] For the ALCCS it may be easier to link the ECD to an elderly (rather than individual sensor devices).

The device commissioning process as described in 3.3.2.2.1 will result in a FHIR resource for the device with a reference to an existing patient FHIR resource that is needed to link the upcoming device FHIR observation(s) resources for monitoring purposes. Alternatively, it is also possible to use a FHIR bundle that contains all information related to the observation(s), but for power and privacy reasons this option is not considered here for IOMT devices.

An Android demo application has been made that scans a QR code containing a device id and a QR code containing a patient id and if valid posts the result as a pseudo FHIR JSON object to a FHIR database that contains the referenced patient resource. An extension to do this demo could be to use the Azure or Google cloud healthcare API and add FHIR observation results from the device. When using Azure, the recently introduced open source FHIR connector for Azure may be used to handle IoMT data in a secure, privacy rules compliant way and to simplify device management.

3.3.2.3 Cellular device operation

The approach described in the previous sections allows large scale deployment of a LoRa device as applied in the ALCCS demo. The use of FHIR resources as described in the previous subsection allows standardized application of such a device in a healthcare environment. Unfortunately, LoRa deployment itself is still limited to a few countries and from business and interoperability point of view it is desirable to have global operating healthcare IoT devices. Achieving this may be possible by using 3GPP standards-based NB-IoT or LTE-M device connectivity instead of LoRa. Further technical differences of using 3GPP connectivity instead of LoRa connectivity were already outlined in D21.4.

When using NB-IoT or LTE-M, pairing from the IoT device to a 3GPP network may be accomplished using eSIM technology. Apart from enabling the global deployment of IoT devices, the eSIM based commissioning of IoT devices will enable hardware-level-security by separating and protecting the storage of symmetric security keys from generic application and firmware. eSIM standards provided by GSMA (GSMA, 2018) ensure cellular grade of integrity protection and tamper-proof physical security features also in NB-IoT and LTE-M implementations.

The following subsection describes how this would change the device commissioning as described in 3.3.2.2.1.

3.3.2.3.1 Device configuration

Unlike existing LoRa based configuration as explained in Section 2.1, the cellular based ElderlyUI will have two key elements on the device required to make a network connection

1. A unique device identity derived from international mobile equipment identity (IMEI)
2. A symmetric network key provided by the network provider which is stored securely in a eSIM.

IMEI is an identity to the cellular modem and the IoT device to which it is integrated. Similar to the mobile communication, NB-IoT and LTE-M will require a combination of IMEI and symmetric network key to securely connect to a cellular network. These credentials are securely stored in an isolated hardware such as a SIM card in conventional cellular communication. The IMEI of the device is a permanent universally unique identifier (UUID) centrally maintained by GSMA. The symmetric keys are issued and maintained by the cellular network provider (e.g. Vodafone) of a device. With the advent of eSIM, secure applications (e.g. signing, hashing, salting, certificate generating etc.) can not only be executed on the eSIM but can also be stored, modified and accessed remotely by an authorized entity with required permissions from the cellular network provider. This enables global deployment of IoT devices with much less logistics required than for a LoRa based deployment.

3.3.2.3.2 eSIM configuration

One of the important features of eSIM is its ability to store value added applications such as encryption and session key generation isolated from the application processor and main memory of the IoMT device. There is no more need for additional network server and network configuration, since the credentials such as AppKey and ASKEY are stored and remotely managed on the eSIM by an authorized service provider. Appropriate service level arrangements with network provider, will not only enable a global connectivity, but also a secure and remote management of the device credentials, firmware and services will be ensured.

Figure 7 shows how the connectivity setup changes for NB-IoT or LTE-M based IoT device with eSIM. Compared to the LoRa based IoT device setup as shown in **Figure 5**, the IoT device commissioning is more straightforward, whereas the security will be improved due to eSIM features as mentioned.

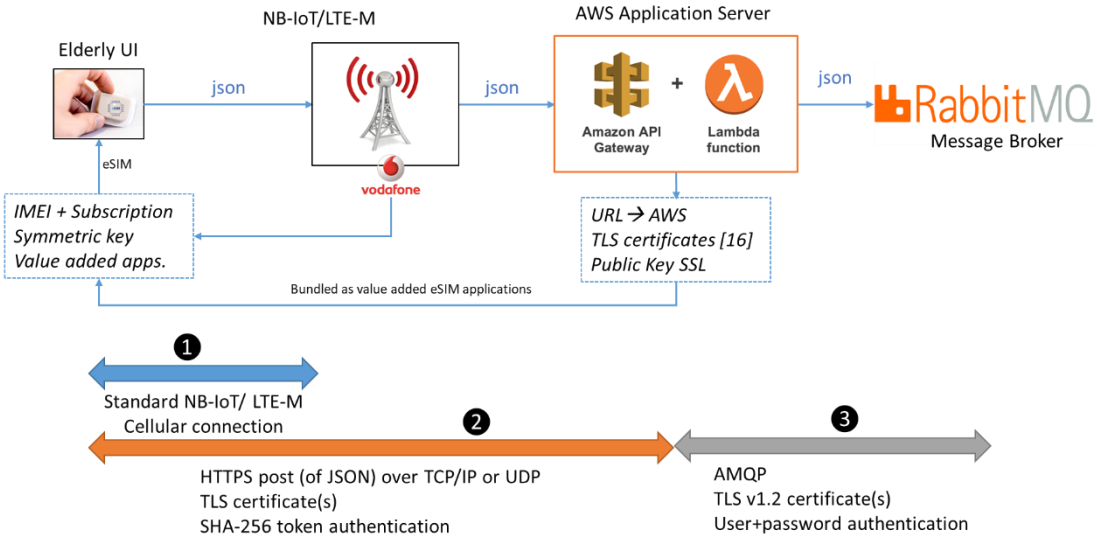

Figure 7: Connectivity setup of NB-IoT or LTE-M based IoT device with eSIM.

3.3.2.3.3 Network configuration

Following the cellular integration, each individual device can be automatically registered to the application server, as soon as it is turned on by an end-user. GSMA has a special provision for global provisioning of eSIM devices known as *Discovery service* [13], which is capable of identifying the un-provisioned eSIM devices as soon as it is turned on and discovered by a base station of any network provider across the globe. The discovery service of the GSMA, being shared service among global network operators, will setup a secure link between the eSIM and the corresponding network operator to securely download the SIM profile to the un-provisioned device. Upon downloading the SIM profile, the IoMT device can connect to the preferred network operator in that geographical area and connect to the application server of the IoT device via internet.

3.3.2.3.4 End-to-end encryption

In addition to the network level encryption offered by the network provider, similar to current version of the elderlyUI, application level end-to-end encryption can be provided as a value-added application in the eSIM configuration.

3.3.2.4 Real Time Location Systems (RTLS)

The elderlyUI is envisioned to support both the indoor and outdoor localization on the device itself and thus the patient that wears it. On-device localization feature of the elderlyUI will complement

and not compete with other existing localization and positioning technologies such as XeTal, YuGen and MPS in the context of ALCCS use case.

Evaluation of localization technologies for the elderlyUI is carried out for two main contexts, indoor and outdoor. For the outdoor localization, use of GPS is avoided because of the high-power consumption and large computational overheads. However, both the LoRa and cellular network provide localization through positioning services with a resolution of 20 meters using Time Difference of Arrival (TDoA) technique in LoRa [14] and 10 meters using triangulation technique in NB-IoT [15]. There are no additional changes required for outdoor positioning in hardware of the elderlyUI since the localization engine will be implemented at the network-end of the NB-IoT service provider and not on the device.

For indoor localization, there are various off-the-shelf technologies available such as Ultra-Wide Band (UWB), Wi-Fi, Bluetooth 5, and optical (e.g. infrared based, visible light based). The addition of new technology for indoor localization requires hardware changes for elderlyUI and infrastructural changes in the care facility, which need to be carefully evaluated against a set of requirements identified for the ALCCS use case. A summary of the requirements of the localization technology identified for the ALCCS use case is provided in [16]. These requirements were also provided as an input for GUT to benchmark their MPS system, which is also based on UWB technology.

Parameter	Use Case Requirements	Based on Bluetooth 5.1 Specification	DecaWave measurements
Localization accuracy	≤ 20 cm for 90% ≤ 30 cm for 100%	≤ 10 cm for 90%	≤ 20 cm for 95%
Localization in horizontal plane	Accurate to floor level	Accurate to floor and room level	Accurate to floor and room level
Robustness	Immune to multipath and human body deviations	Sensitive to multipath Less sensitive to human body	Immune to multipath Sensitive to human body (e.g. wearables)
Security	PHY layer	Prone to replay attack	Distance time bound protocol
People tracking	Latency ≤ 1 second.	Latency ≤ 100 ms (no implementation available yet)	Latency ≤ 100 ms (12 s measured for initial setup, and 1-2 s delay for updating location in live-tracking)
Asset tracking	Latency ≤ 5 minutes	Latency ≤ 100 ms	Latency ≤ 100 ms (12 s measured for initial setup)
Battery life time of Tag	rechargeable: 7 days, non-rechargeable: 1 year	Up to 10 years (CR2032 – 0.1Hz update rate)	Up to 7 years (CR2032 – 0.1Hz update rate)
Hardware Cost (anchors, hubs …)	≤ $150 per room	No product available yet	≤ $100 per room
Installation Cost	≤ $100 room (20m^2)	t.b.d.	≤ $50 room (20m^2)
Technology	Wireless	BLE (with angle of arrival)	UWB
Frequency	Regulated ISM	2.402 GHz to 2.480 GHz	6.240 GHz to 6.740 GHz
PHY Data rate		2 Mbps	6.8 Mbps

Table 1: Localization Requirements, specifications and evaluation.

3.3.2.4.1 Evaluation of DecaWave for RTLS

Based on these requirements and availability of the off-the-shelf hardware, DecaWave tags were chosen to be empirically evaluated within the context of D21.6. DecaWave evaluation kits [17] implements two-way ranging technique, in which the tag successively sends messages to each of the anchors in sight and receives an acknowledgement immediately. By measuring the round-trip delay (considering the fixed time needed by the anchor to acknowledge the tag), the distance to

each anchor from the tag can be computed either on the tag or on the anchor. We chose the office environment which closely resembles an elderly care facility with rooms of resembling size as shown in Figure 8.

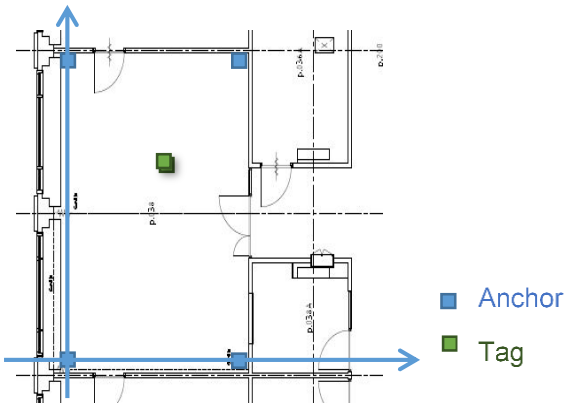

Figure 8: Office room for setup of empirical evaluation

4 DecaWave devices were configured as Anchors and were installed in a room of 30m2. These anchors were connected to mains supply and are attached to the wall at a height of 2 meters ensuring line-of-sight between the anchors. These anchors can be connected to Ethernet and powered using power over Ethernet (PoE). However careful consideration of the location of these anchors in a room is needed which requires in-depth analysis of the layout of the room in a building.

A DecaWave tag, resembling the elderlyUI, supports both UWB and Bluetooth. The localization engine uses UWB technology and the data communication between the tag and an Android tablet uses Bluetooth. The system level architecture of the DecaWave systems is shown in *Figure 9*. It also shows a person wearing the DecaWave tag. This is a scenario resembling a body-worn elderlyUI in order to measure the impact of the human body in UWB and the localization engine.

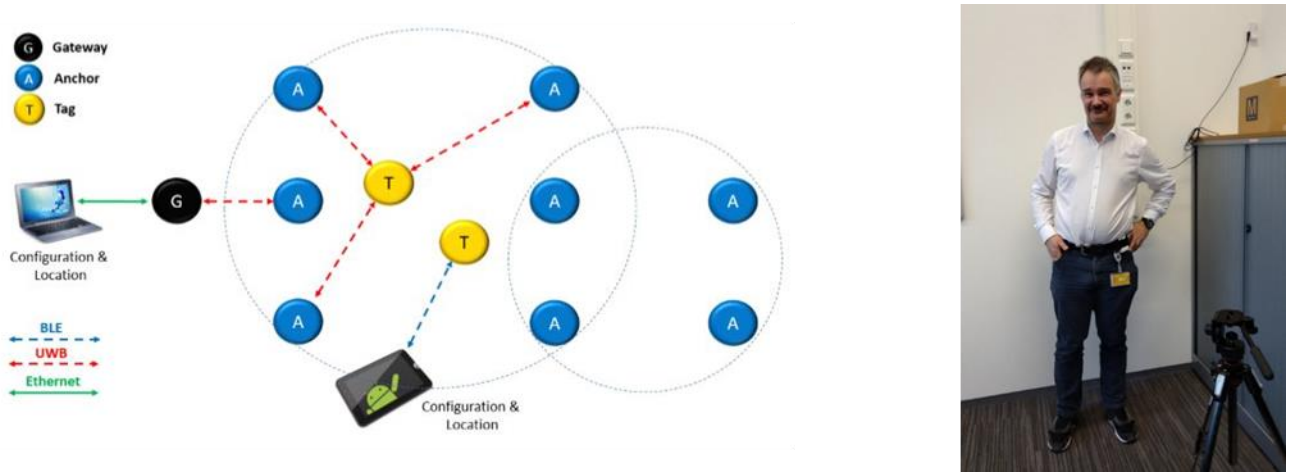

Figure 9: System architecture of DecaWave and on-body testing of DecaWave tags

3.3.2.4.1.1 Conclusions from RTLS evaluation for deployment in elderlyUI

The positioning accuracy is generally better than the stated requirements of 30 cm. However, in situations with poor line-of-sight, the accuracy is reduced and could be as bad as 1 m.

In realistic scenarios there might be higher objects (e.g. metal closets) blocking line-of-sight also at 2 m height. Unexplainable large deviations occurred temporarily during the “close to anchor” tests at 1 m height. This may be an indication that the chosen implementation (i.e. DecaWave’s algorithms)

is not completely robust under all circumstances. Further optimization of the localization engine for use case specific implementation will be required.

Proper antenna design taking into account the RF impact of the human body is essential, both from a communication and localization point-of-view.

3.3.3 Vemco

In the third iteration of WP21, Vemco was working on improving security of its Access Control System with respect to the SCOTT's Security Scan results [14].

3.3.3.1 Security

Vemco focused mostly on the security of:

- services in the cloud;
- the edge nodes;
- link between edge and cloud.

Vemco is the main integrator in WP9, WP15, and WP21, it provides the RabbitMQ message broker accessible for all the partners. In order to not interrupt partners' work, Vemco introduced and tested all the security improvements only on a local copy of the server infrastructure.

Secure element

Vemco has searched for suitable hardware chips which would allow for symmetric / asymmetric hardware encryption using securely stored keys, secure authentication, and preventing software piracy on the edge. Cloud platform vendors' support for provisioning and authorization was also taken into account. Finally, four Microchip modules were chosen for further tests and analysis:

- ATECC608A
- ATECC508A
- ATSHA204A
- ATAES132A

The first part of tests included studying of documentation and use cases was provided by Microchip to acquire knowledge needed to incorporate modules into Vemco's solution in a thoughtful way. Vemco is now working on implementing the authentication mechanism between edge and cloud services with securely stored credentials/keys.

Important note

Vemco had planned working not only on the security of cloud and edge, but also on the security of its BLE lock. However, its development had to be discontinued. The initial decision on taking up a development of a proprietary mobile authentication was based on the analysis of the market made prior to the SCOTT project. Since then, the main locks/readers vendor changed its pricing plan significantly. Therefore, a justification of the business case is not valid anymore. Access Control System was designed to be able to handle both proprietary and off-the-shelf mobile authorization solutions, so consequences of the change for the project are negligible.

3.3.3.2 Access Control System – GUI

As defined in the deliverable D21.5, Vemco's goal for the last WP21 iteration was to prepare a graphical user interface for the Access Control System (ACS), a part of BB23.P. To understand why

the UI has been designed in a way presented below, the reader must know that apart from WP21, BB23.P is used in WP9 and WP15. There, ACS is developed to meet requirements of large industrial facilities like refineries or chemical plants. However, the system can be scaled down and applied in smaller and simpler use cases like this presented in the ALCCS demonstrator.

In the period covered by the report, Vemco prepared dozens of user interface mockups covering the functional scope of the ACS in the project. Implementation of the mockups has started and will be continued until the very end of the project. A series of screenshots of already implemented application views presenting the flow of the ACS management in the WP21 can be found below.

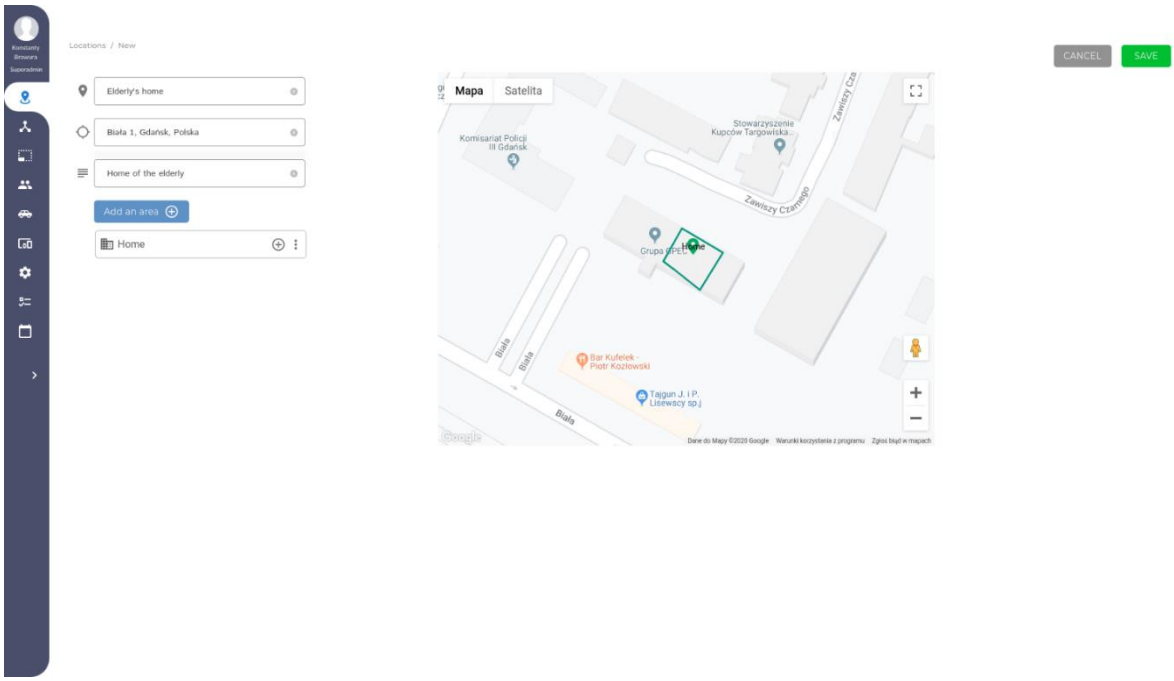

Figure 10: Adding an elderly's home in the app

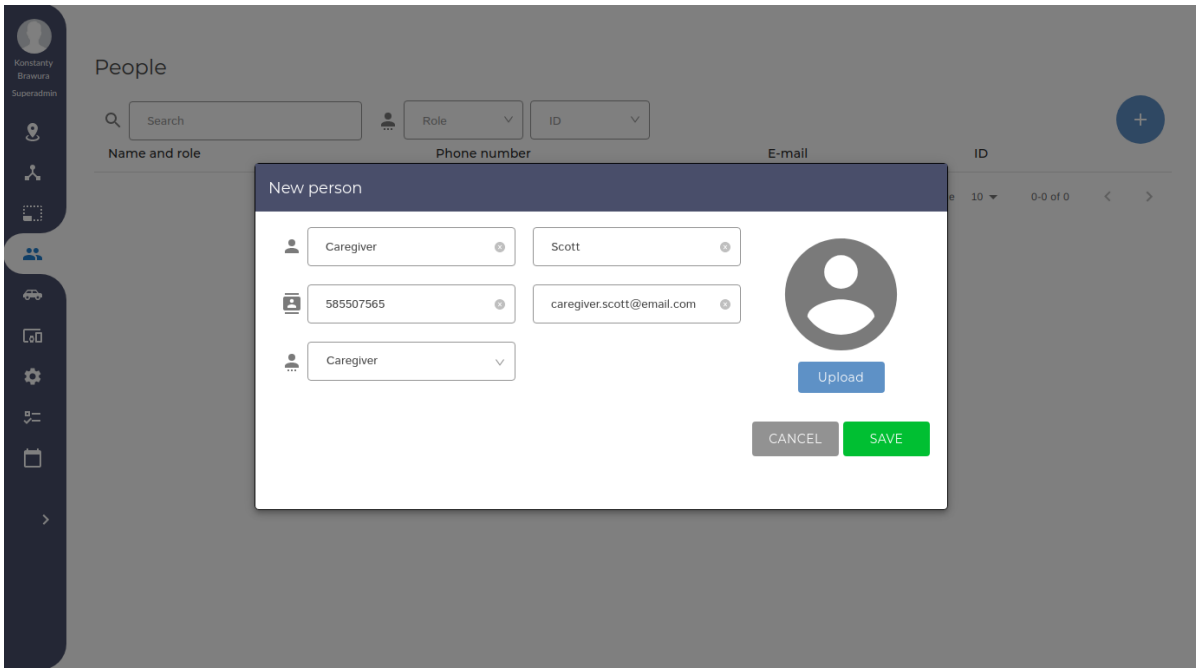

Figure 11: Adding a caregiver

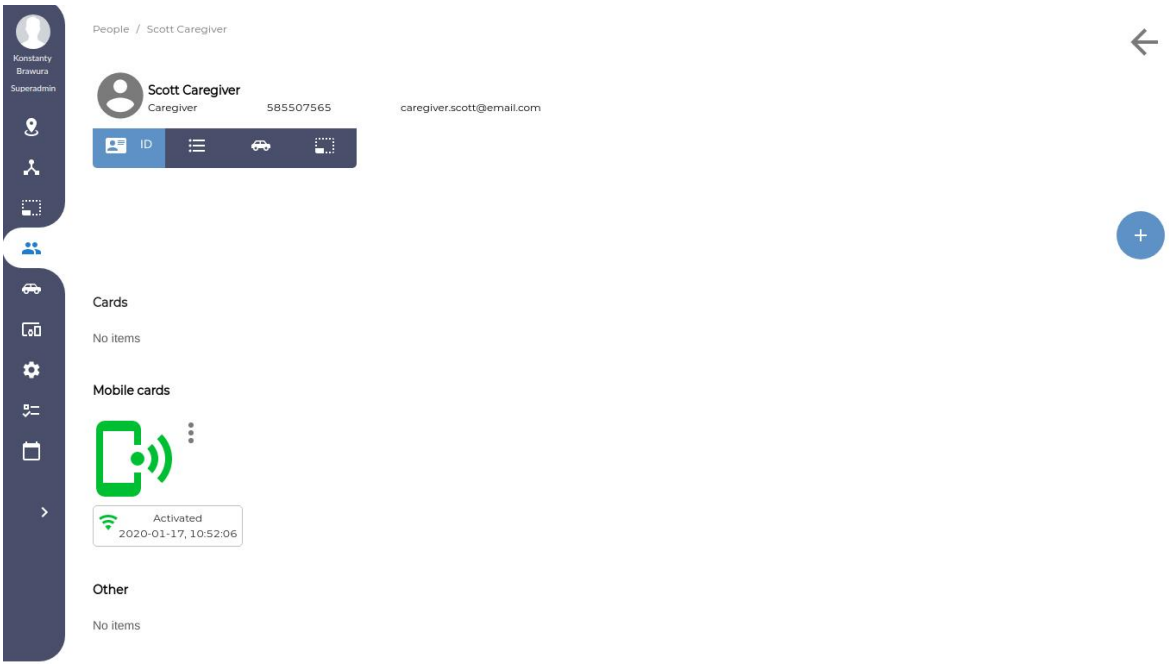

Figure 12: Showing a caregiver with an activated mobile access card

3.3.4 GUT

In the previous iterations, GUT installed its Multimodal Positioning System (MPS) in the WP21 demo site in Eindhoven. However, the system was not working properly, what was described in deliverables D21.4 [2] and D21.5 [1]. Therefore, the main goal for the third iteration was to fix the MPS and integrate it with the rest of the system. Other goals were related to improvements needed to increase system maturity.

Fixing the stability problems

GUT conducted a series of tests to find a root cause of problems of the MPS setup in Eindhoven. Malfunctioning of the system was caused by problems with power supply section of the MPS Gateway module. The design of MPS Gateway printed circuit board was altered and new modules were manufactured. Moreover, instability in communication between chips inside the MPS Gateway was found and fixed.

Remote updates

Since GUT is continuously improving its system, a mechanism for updating its instances remotely is required. In the third iteration GUT prepared CI/CD pipelines for updating:

- Localization algorithms;
- Wi-Fi capable chips on the MPS Gateways;
- BLE capable chips on the MPS Gateways;
- Management app – both frontend and backend.

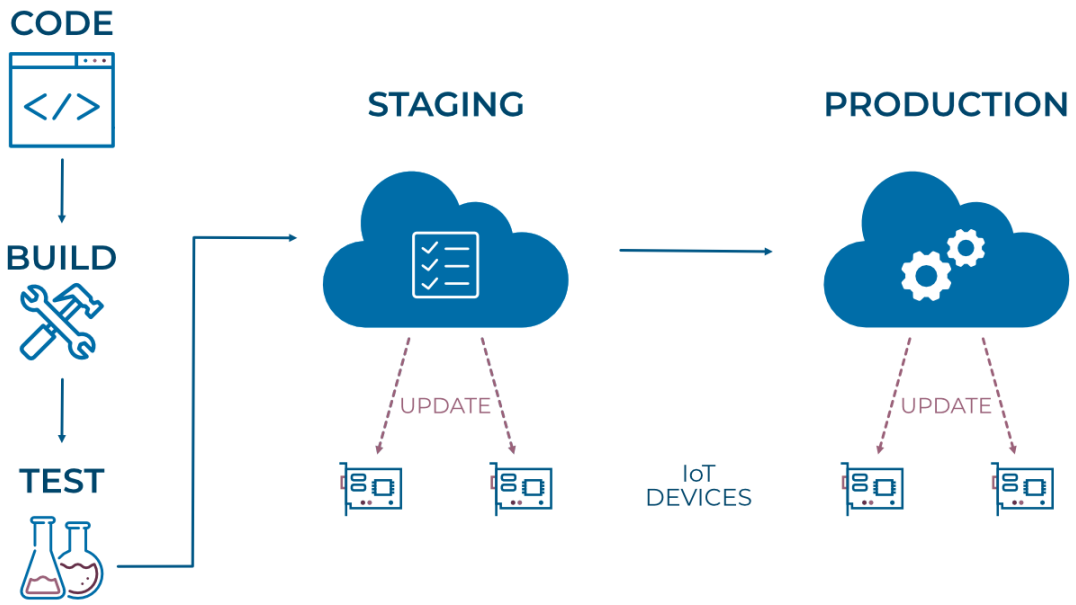

Figure 13: CI/CD pipelines - MPS

Localization accuracy

Localization accuracy achieved during the first deployment in Eindhoven was below expectations. In the third iteration GUT improved it by fine-tuning of the algorithms and change in position reference nodes – now they are attached to the wall, not to the celling as previously. Moreover, GUT solved a problem of 'jumping dot' on a map by introducing Kalman filtering.

Deployment in Eindhoven and integration with the ALCCS

In December 2019, GUT visited TU/e and upgraded the MPS entity there. Since January 2020 measurements from the MPS are being routed to the Elderly Context Derivation engine. There, the measurements can be used as an additional factor in making decision about raising an alarm.

Figure 14: MPS entity in TU/s building in Eindhoven - UI screenshot.

3.3.5 Xetal

As indicated in the previous deliverable [1], Xetal has been working on a new type of sensors and first prototypes have already been shown at the end of 2nd iteration. Initially 3 prototypes were shown (Figure 15) with three different Field of View (FoV: 40x120, 90x90 and 105x105 degrees) powered by a Microchip PIC microcontroller. As indicated in the previous report, a second batch of prototypes was made for a version of the same three sensors but powered by a Microchip ARM core for more complex data analysis.

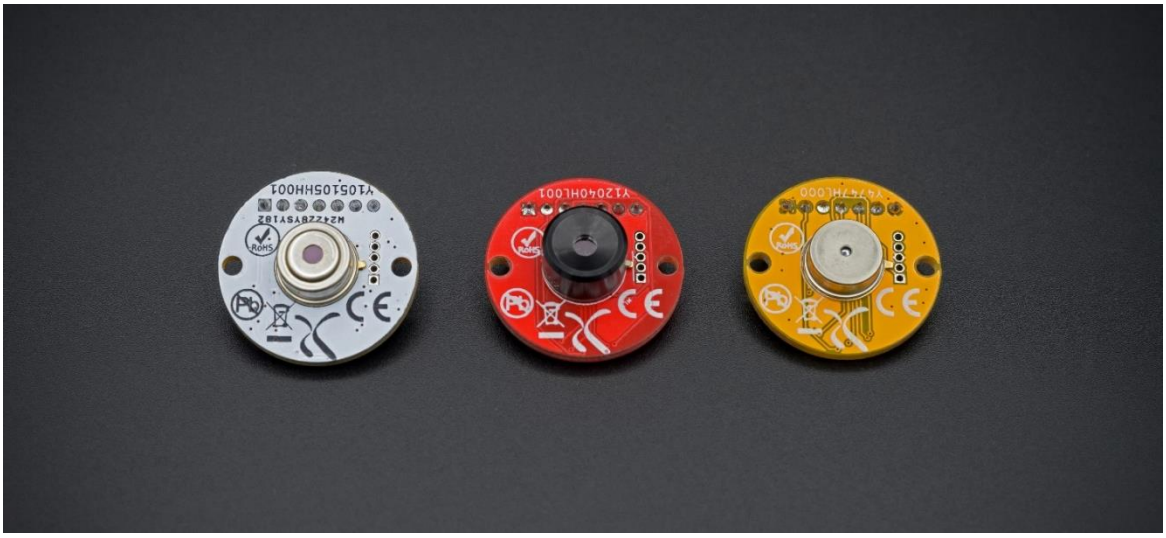

Figure 15: First Xetal Yugen sensor prototypes differing in area coverage, processing power and acquisition speed.

The initial prototypes were functional but proved somewhat unstable due to design errors. Since then, 5 more design iterations have been done. The final versions of the Yugen sensor family still includes three sensor models (with different field of view) but in four variants: powered by a Microchip PIC microcontroller, powered by a Microchip ARM microcontroller, with an additional light sensor (for measurement of color and intensity of light) or without. The standard form factor has not changed from what is shown in Figure 16 and an expansion port has been added in order to add modules for wireless communication or additional computational capabilities.

The redesigns have not only focused on hardware redesign, but also on the embedded software. Currently each sensor can achieve an accuracy of at least 96% (in real life testing), which is sensibly better than the maximum accuracy obtained with high-end AI Cameras (82% in artificial and controlled testing). We have achieved this result by redesigning completely the algorithms that were being used initially. We believe that we have achieved almost the maximum quality of data possible with the currently available temperature sensing element used in our sensors. After the end of the project we will consider further improvement by means of collaboration with third parties for designing a dedicated sensing element, which should allow accuracies in the order of 99%.

Figure 16: Latest Xetal Yugen prototype (40x120 FoV) inclusing a wireless module connected to its back.

As illustrated in the ALCCS demonstrator, one sensor can be used to detect and localize people in room size areas (depending on the selected FoV and height of installation). However, in order to monitor large areas, it is important to have multiple sensors working together as if they were a single sensor (i.e. a sensor network). In this way it is possible to detect, localize and track people in buildings and office areas.

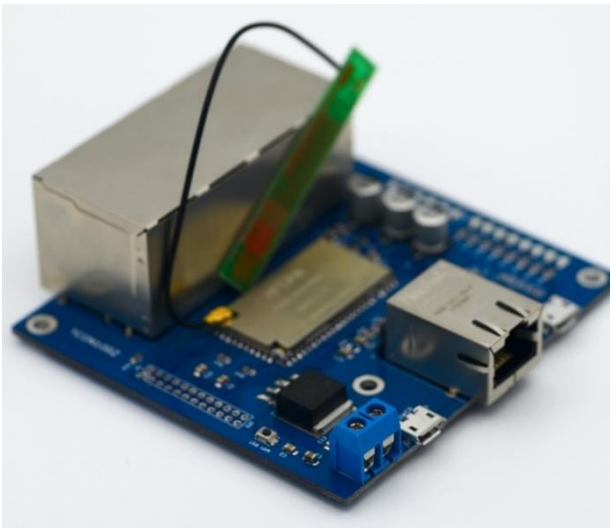

Figure 17: Xetal Yugen Hub used to aggregate data from several sensors and upload it to the Yugen Fusion Server.

In order to achieve this goal, we have defined and build a Yugen system based on a simple star network topology, where each sensor sends its localization data to one aggregator or Hub (Figure 17). The Hub collects the data and send it to a server (i.e. Fusion Server) which fuse the data and makes it available in various format (such as the JSON format already agreed and used for previous demonstrator). Such a Fusion Server acts as a single sensor even if it is actually using any number of physical sensors. Each Hub is designed to be capable to collect data from up to 16 wireless sensors (Wi-Fi) and 32 wired sensors. The Server runs on any conventional hardware be it a PC or else. This architecture has been tested in-the-field to up to 40 sensors distributed across different floors and up to 10 Hubs. A first large (commercial deployment) of 100 sensors across an entire building is scheduled for spring 2020.

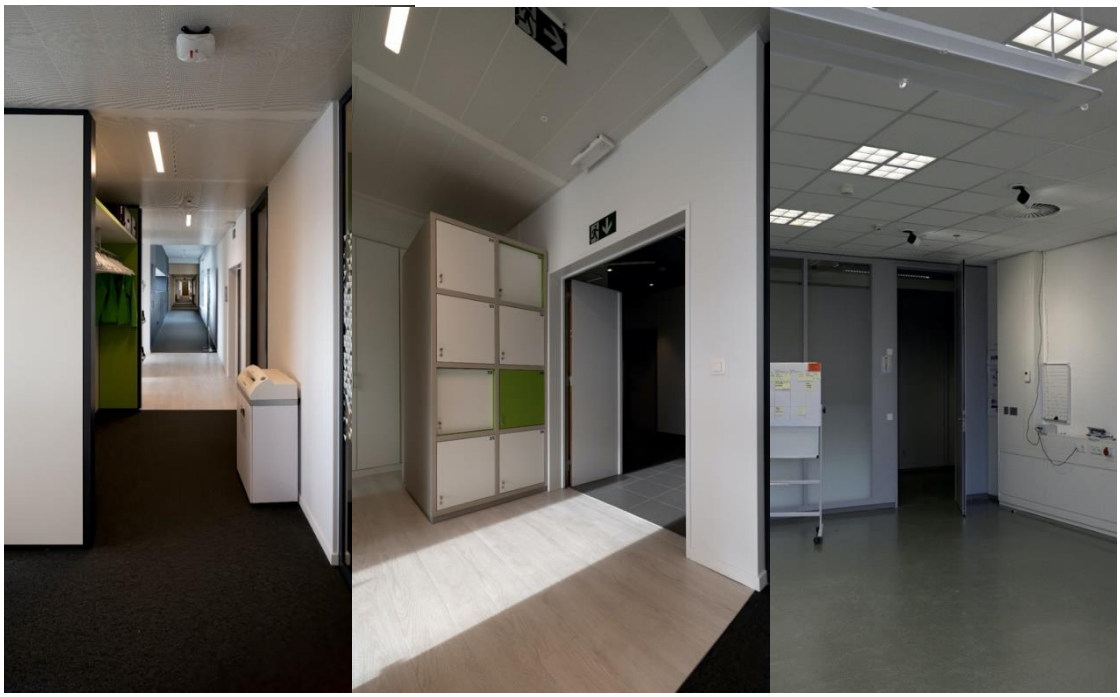

Figure 18: Example of installation for development and testing of multiple Xetal Yugen sensors connected in a network.

The sensor network has been developed and tested in this 3rd iteration with the collaboration of several of our partners in various situations (such as building control, meeting room occupancy detection, laboratory usage, school restroom monitoring, etc). Figure 18 shows some examples of areas where sensors where installed and also illustrates how well the sensor blend in the building. They are virtually invisible.

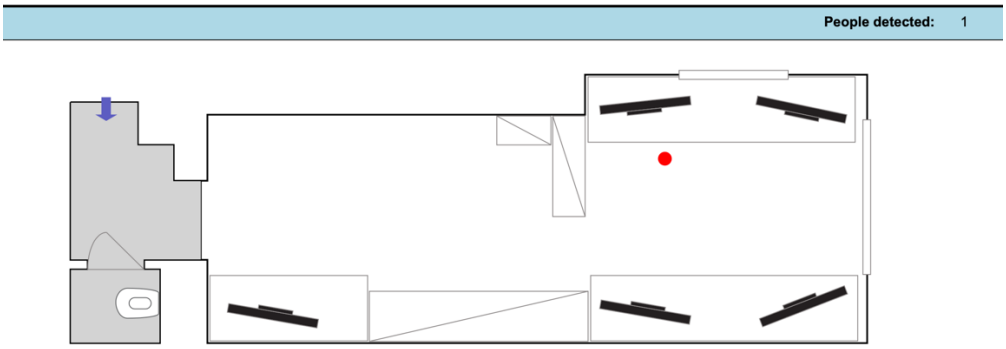

Figure 19: Example where the data from a network of 6 Yugen sensors is used for monitoring an office floor.

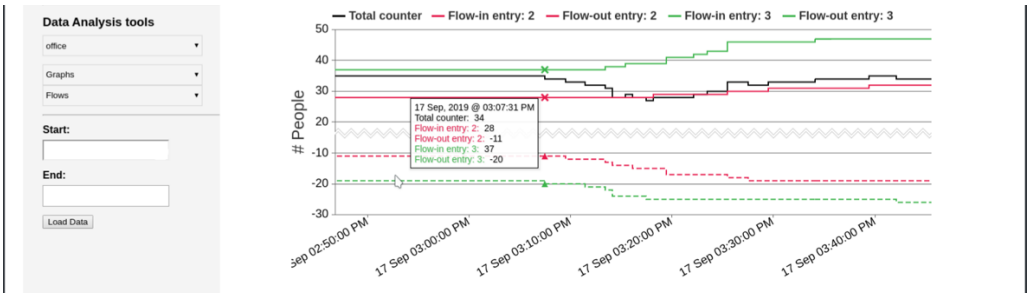

Figure 20: Example data the server provides out of several Yugen sensors in a building in order to provide information about flow and presence of people in a given area.

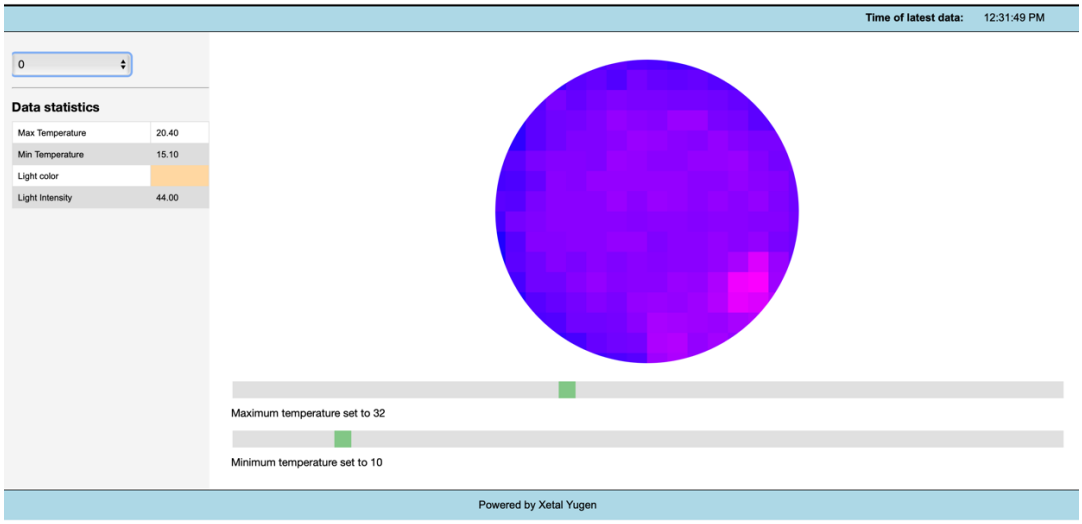

Figure 21: Example of thermal map provides by the server for a sensor used to monitor a meeting area.

The test have shown that a network of Yugen sensors can detect and localize people (Figure 19) as well as provide other data such as people flow (Figure 20), thermal maps (Figure 21), thermal anomalies, etc. with an accuracy of at least 95% even when the sensors have a non-perfect area coverage (due to practical issues unavoidable in real world installations).

3.3.6 UiO

UiO has extended the Attribute-Based Access Control (ABAC), which was implemented on a cloud server before, with a Semantic Attribute-Based Access Control (SABAC) that makes a decision semantically and considers the semantic relationships for inferring new policies (i.e., implicit policies). The SABAC is developed by integration of semantic technologies with the previous ABAC engine. As shown in Figure 21, SABAC, as a cloud service, makes a decision not only based on access control policies and subject, object, environment's attributes, but also based on an ontology representing the semantic relationships between attributes.

The rationale behind the integration of SABAC (instead of ABAC) was to improve the scalability, dynamicity, security, and the precision of the access control mechanism. Now, SABAC allows caregivers from different domains (e.g., different countries or institutions) to help elderly people in the case of emergencies without the need for translating their certificates, attributes, and so on. For example, a Norwegian caregiver who has an attribute named "Lege" can manage an emergency in, for example, US, which only caregivers who have an attribute named "Doctor" can help.

Due to the integration with Vemco's physical access control module, we have changed the message formats (i.e., access requests/responses) from XACML to JSON. UiO has also made a video for standalone demonstration for SABAC.

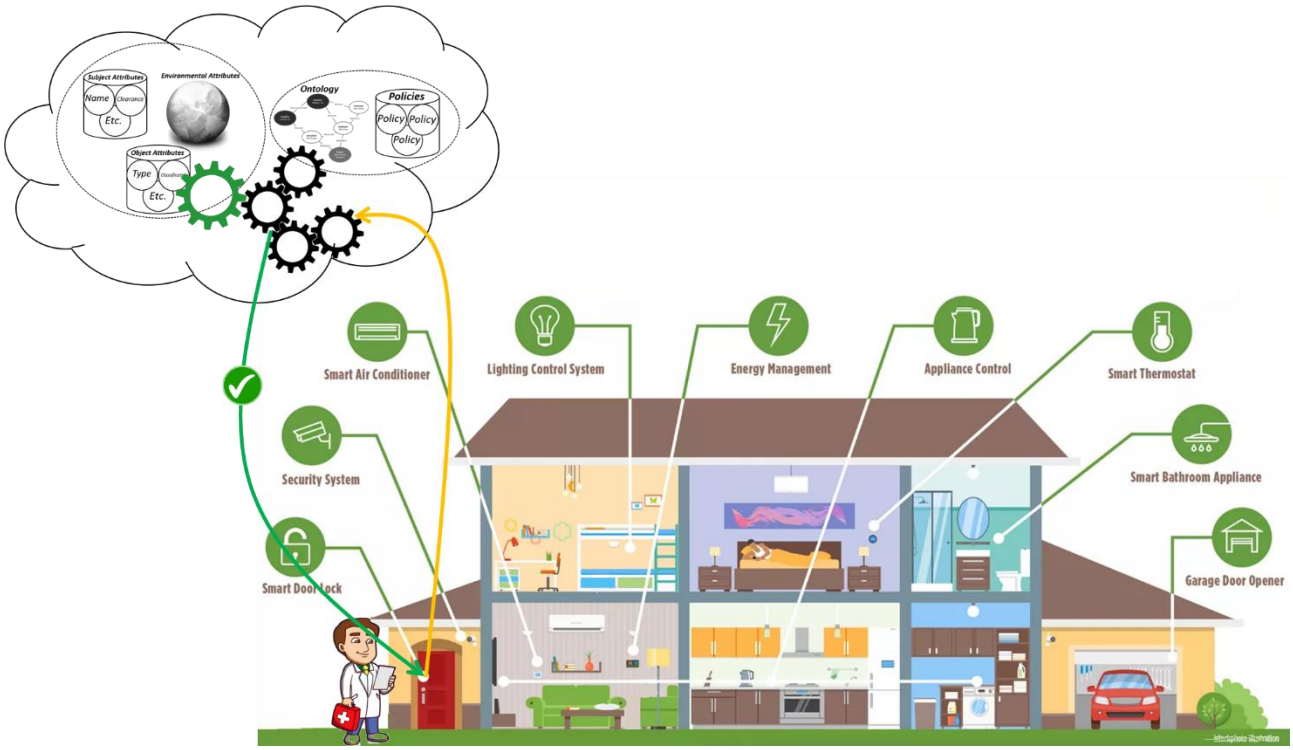

Figure 22: The overall schema of applying SABAC in WP21

3.3.7 Tellu

Tellu has improved the diabetes sub-system of the demonstrator according to the plans set out in D21.5. The target group is elderly residents with diabetes type 2. The diabetes sub-system consists of:

- Medical sensors (measuring blood glucose, blood pressure and weight)
- The Tellu Medical Gateway app running on a smartphone
- Integration with the ALCCS message broker to send important events to the Elderly Context Derivation
- Integration with TelluCloud for use in medical services.

Three features were identified for improvement in D21.5, the work done for each of these is described in the following subsections.

3.3.7.1 Medical devices / BioMKR

D21.5, section 3.5.7.1 discusses issues with the BioMKR continuous glucose monitoring prototype device, which is used in the demonstrator. Since this was still a prototype that is unavailable for other partners or commercial use, we have assessed alternative devices for doing continuous glucose monitoring.

The state-of-the-art commercial alternative currently, is the Dexcom G6 (https://www.dexcom.com/). This continuous glucose monitoring device is now available in Europe. It uses a physical sensor which is inserted under the skin. The user inserts the sensor on the stomach with an applicator. It has a patch with connector, and a small transmitter is plugged in, to connect the sensor to a phone running an app. The sensor must be replaced with a new one every 10 days. So, it is intrusive, and

quite expensive if not subsidized by public health plans (for instance, a 12-month contract is offered in the UK for £159/month).

Figure 23: Dexcom patch with sensor (top left) and applicator.

Dexcom does not provide direct access to the device for developers, so it is not possible to integrate the device with the Tellu Medical Gateway app in the way it was done with the BioMKR. All data from Dexcom devices go through the Dexcom cloud. An API is provided for the cloud side, allowing third-party developers to make apps for Dexcom users that support access to their Dexcom data [https://developer.dexcom.com/]. This is a REST API with OAuth 2.0 authentication.

The Dexcom G6 is potentially interesting for future commercial exploitation of the diabetes sub-system. However, we have not pursued it further in the SCOTT project. The decision is based on a combination of not being able to integrate it directly on the client side (where Tellu is doing the main SCOTT effort), to ensure that data is not shared with third parties, and due to time constraints. The BioMKR prototype therefore remains the continuous glucose monitoring device for the ALCCS demonstrator.

3.3.7.2 Tellu Medical Gateway app

A new version of the app has been developed, refactored to use the latest versions of Tellu libraries and Xamarin Forms (https://docs.microsoft.com/en-us/xamarin/xamarin-forms/). The most important addition is session handling with authentication for the new TelluCloud FHIR API. This is the App-TelluCloud connection described in the next section. A status screen has also been added to the app, to give detailed status information and help diagnose problems in a user-friendly way.

This provides a final version of the Tellu Medical Gateway app. The app can be connected to either the ALCCS message broker or to TelluCloud. The TelluCloud connection requires authentication as a registered user. The app provides Bluetooth device pairing with the medical devices and reads device measurements. It also has a demo mode generating raising and falling glucose measurements, to test and demo triggering of alerts. *Figure 24* shows some screenshots from the app.

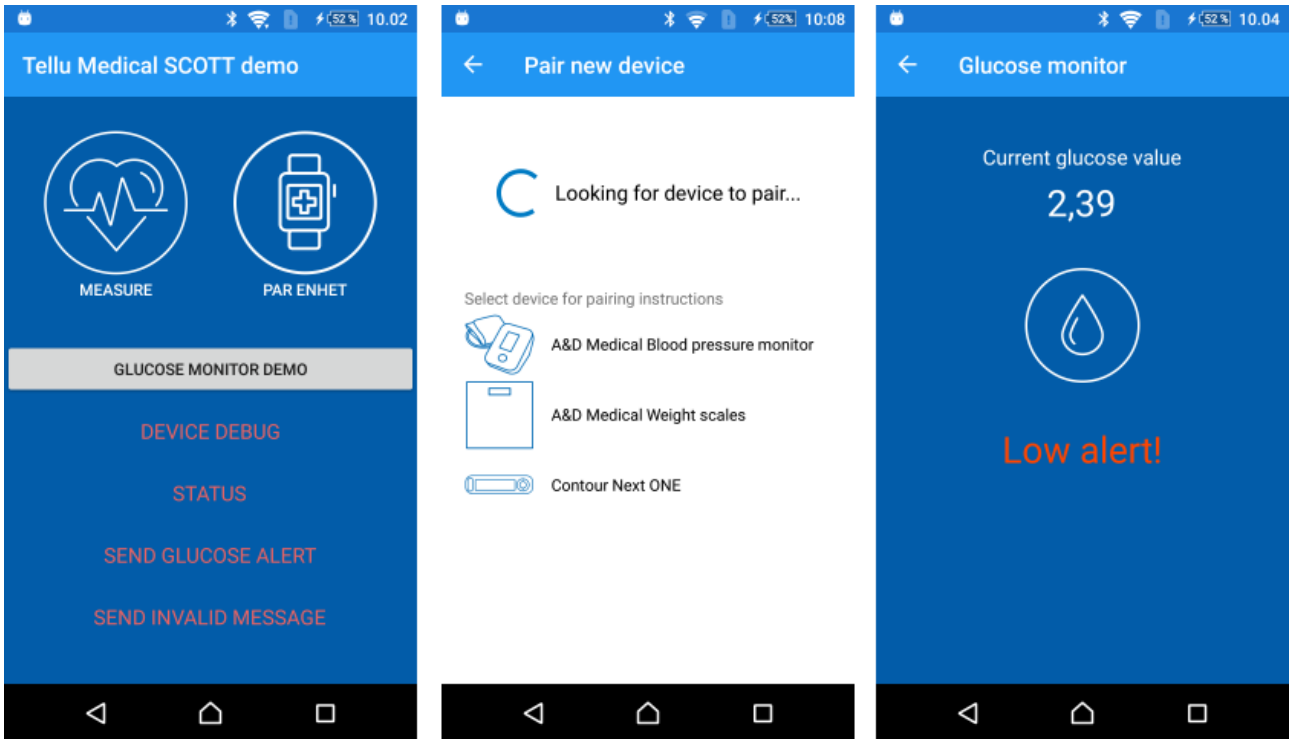

Figure 24: Screenshots from the Tellu Medical Gateway app.

3.3.7.3 App-TelluCloud connection

Tellu's cloud platform, TelluCloud, now has an API to receive medical data in FHIR format [11]. FHIR is a standard for exchange of medical data, and use of FHIR facilitates integration of TelluCloud with medical back-end systems. Users are modelled as patients in the FHIR service, and to use the app with the TelluCloud connection you need to authenticate as a registered FHIR patient. Measurements are posted to the API as FHIR Observation objects.

Along with the FHIR API, TelluCloud has a new authentication broker based on OpenID Connect. A token from this broker is needed to use the FHIR API. TelluCloud Authentication Broker federates identities provided by other federation services and identity providers. By using the standardized protocols OpenID Connect v1.0 (https://openid.net/specs/openid-connect-core-1_0.html), TelluCloud Authentication broker can provide identities from a set of federation services and identity providers, including:

- ID-porten: ID-porten is the national identity federation service in Norway that provides identities verified by five different identity providers: MinID, BankID, BankID on mobile, Buypass or Commfides. Identities provided by ID-porten must only be used by public services, or service providers operating on behalf of a public service.
- HelseID: HelseID is an identity federation service provided by Norsk Helsenett for authenticating health personnel in Norwegian e-health solutions. HelseID federates identities from regional health organizations, local identity providers and ID-porten. In addition, HelseID will enrich the identity with information about the user from Helsepersonellregisteret and Personregisteret.
- Social Identity Providers: TelluCloud Authentication Broker can also be configured to federate identity from social identity providers. Currently a number of social identity providers are supported, such as Facebook, Google, LinkedIn, Microsoft, Twitter and PayPal.

Tellu also has sub-contractors to federate identities from ID-providers outside of Norway, including providers in Nordic countries and a set of countries in the EU.

The process of authenticating a user is implemented using the OpenID Connect v1.0 protocol. OpenID Connect is an authentication layer on top of the authorization framework OAuth 2.0. The protocol defines a set of different authentication flows, where the choice of the used flow typically depends on the type of client application and type of user that will be authenticated.

To connect to TelluCloud, the mobile app user must authenticate in the web interface of the TelluCloud Authentication Broker. Based on the type of ID used, this could be two-factor authentication. For test and demonstration, we have mainly used our own Tellu ID, as this is a simple username and password login. When designing this aspect of the mobile app, it was important to study and follow current best practices (https://tools.ietf.org/html/rfc8252). Many apps have used an embedded web view, so that the web page is shown within the app. This is not good practice, as it allows the app to gain access to the user's input in the web page. The current best practice is to use the external browser component in the device, invoking this from the app and having it redirect back to the app with credentials once the authentication is completed. Protocols for this are implemented on all recent versions of both Android and iOS.

To implement the protocol in the app, we found a C# library supporting Xamarin apps: IdentityModel.OidcClient2 (https://github.com/IdentityModel/IdentityModel.OidcClient2). This OpenID Connect Client Library is open-source and certified by the OpenID Foundation. When selecting "Connect to TelluCloud", the browser opens on the TelluCloud Authentication Broker URL setup for this application. The user authenticates in the web interface, and is redirected back to the app, which receives the token. The token is stored in encrypted storage, so that the user does not need to re-authenticate while the token is still valid. Tokens have a short lifespan, as set by the service that issues them. When no longer valid, a new authentication may be required (the protocol also supports a separate refresh token with a longer lifespan, which can be used to get a new authorization token). Managing the session takes some care, and we need to remember that it is managed separately by the browser and by the app. The browser stores its session, so if the app invokes the browser to do authentication while the browser still has a valid session, it will redirect directly back to the app with the current credentials, not allowing any user interaction. So, the app provides a logout option that allows the user to terminate the session. This invokes the browser through the OidcClient library, returning to the app when the logout transaction is completed.

Figure 25: TelluCloud ID authentication in browser.

3.3.8 Telenor, OsloMet and Wolffia

Telenor, Wolffia and OsloMet introduced network slicing at the network layer to the existing ALCSS use case of WP21.

A flexible and secure integration of connected devices into established healthcare scenarios is crucial for the acceptance of IoT in the healthcare industry. The coming 5G mobile network technology would provide many solutions to the challenges of security and trust in deployment of IoT in health care.

Telenor, Wolffia and OsloMet have continued with the research tasks mentioned in D21.5 and focused their work on the improvement of our demonstrator of the scenarios that were illustrated in D21.4, which is available in a video format.[2] The demonstrator elaborates on how network slicing can be achieved while considering previously mentioned aspects such as authentication and identity management of both users and devices relating to the ALCSS (i.e. “main”) use case of WP21.

More specifically, during the third iteration, Telenor, OsloMet and Wolffia continued the implementation and specification of 5G Slices. In that regards, the two network slices have been implemented: one for assisted living devices and one for healthcare center of the existing ALCSS use case of the work package. These two network slices can be customizable within the scope of the Kubernetes cluster (https://kubernetes.io/) in which the containers are running and the FlexRAN controller (as depicted in the figure below).

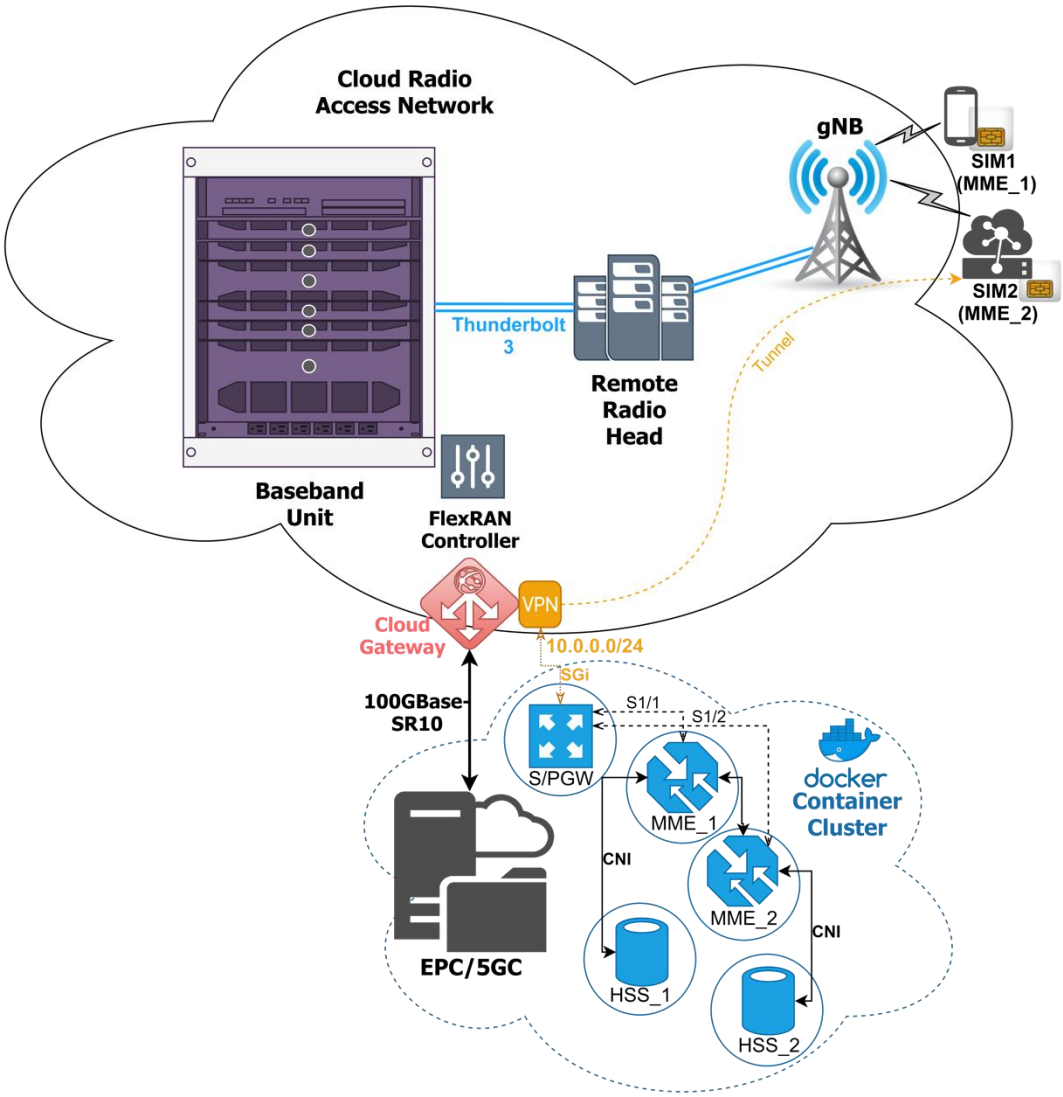

Figure 26: Network slices

[2] https://www.youtube.com/watch?v=4SDFj059AhY

The 5G network is deployed according to 3GPP Option 7 CU (Centralized Unit) – DU (Distributed Unit) split, where the functionality of the Remote Radio Heads and Baseband Units is detached in different datacenters/servers and the gNB base station is instantiated locally on a PC. The container cluster is regulated in that manner. It employs multiple different containers for different modules of the core network, allowing for CI/CD (continuous integration / delivery) paradigm enforcement, as well as service-based architecture, i.e. micro-services. The FlexRAN controller indicates two network slices according to two distinct MMEs (Mobility Management Entities), which authenticate two different sets of users in the HSS database (Home Subscriber Server), that is in 4G LTE terminology as we do not have the 5GC (5G Core) deployed yet.

Users with SIM1 cards will authenticate to the MME_1, which will allow for regular cell-phone attachment and usage, whereas IoT devices and gadgets will utilize SIM2 and will be handled by the MME_2, which will have a different quality of service and allow for different set of UE (User Equipment) in the HSS_2 database, correspondingly.

To demonstrate also a level of security, this architecture allows for implementation of VPN encrypted tunnels, which will enhance the security of devices attaching to a core network deployed in a shared cloud environment (i.e. Amazon Web Services – AWS).

At this point, the two slices can be regarded as isolated, with different broadcast domains and addressing, as well as policy enforcement regulated in the container network interface (CNI), by using the Calico plugin for Border Gateway Protocol (BGP) networking in Docker containers. This policy enforcement dictates the viability of connection to external networks, as well as inter-container communication, allowing or disallowing particular parts of the core network modules to be connected to their corresponding instances. For example, MME_1 Docker container can only communicate with HSS_1 Docker container that is for correlating users with SIM1 that need to attach to the first network slice. On the other hand, the MME_2 will only be able to communicate with HSS_2, in which the UE with SIM2 will be attached. At this point, the MME_1 cannot communicate with HSS_2, even if the broadcasting domain is the same, as the policy indicated in the BGP routing tables will disallow communication to the same.

With this architecture, we have demonstrated isolation of two different network slices using the Kubernetes container orchestrator, providing in parallel a robust and simple way of managing large-scale networking in cloud environments for mobile communication systems such as 5G.

Our aim hence forward is to continue to improve our solution as we consider the inclusion of various devices and see the interoperability between the two aforementioned slices, being one dedicated for the assisting living devices and the other for the healthcare services.

4 EMERGENCY DEPARTMENT EQUIPMENT AND PATIENT TRACKING USE CASE

4.1 Context of the use-case

In the first year of SCOTT, one of the actions taken by GUT was stakeholder involvement. Its goal was finding opportunities to use technologies developed in WP21 in many health contexts. As a result, cooperation between GUT and *Copernicus*, a hospital network in northern Poland, has been established. In the *Copernicus* network, around 3000 patients are treated.

Figure 27: Emergency Department Equipment and Patient Tracking Use Case – Overview.

4.2 High level architecture of the Use Case components

Figure 28 presents mapping of the Multimodal Positioning System for the SCOTT reference architecture, in particular for the physical entity model. Reference and Localized nodes are on the

Layer 0, in the hospital bubble. Devices on the Layer 1 are gateways between the hospital bubble and the private or public cloud which is Layer 2.

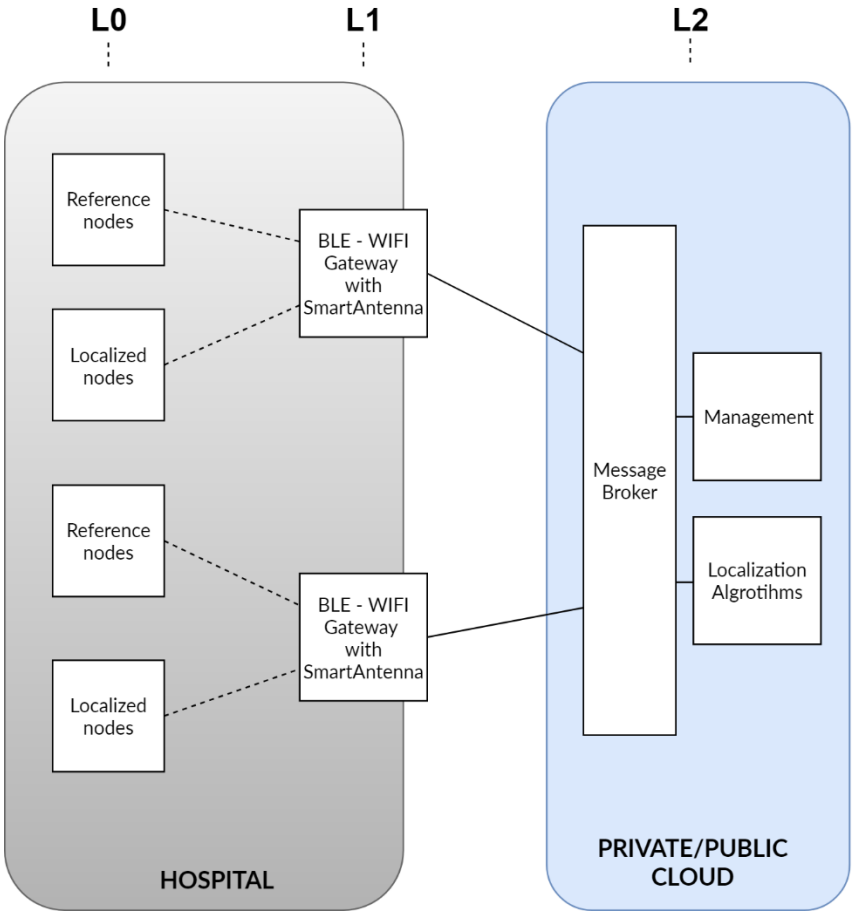

Figure 28: HLA - Physical entity model

Reference nodes – BLE beacons with fixed position handled as reference points.

Localized nodes – BLE beacons used to localize medical equipment and patients with dementia.

Gateway – BLE-WIFI Gateway equipped with the Smart Antenna (for details please refer the previous deliverables).

Message Broker – MQTT-based message broker.

Management – cloud-based app responsible for management and device provisioning.

Localization Algorithms – cloud-based app calculating beacons' positions.

4.3 Achievements

In the third iteration, GUT decided to alter its plans regarding a pilot deployment in the emergency department of one of the hospitals in Gdansk. Previously, GUT planned to prepare deployment of MPS by the end of the project (refer to D21.5 [1] for more details). GUT decided, however, to introduce an additional step before installing any hardware in the hospital. This step is a demonstration of the agreed scenarios to both the stakeholders and the end-users in the GUT's building. It would allow to get feedback and introduce appropriate adjustments before interrupting the work of the Emergency Department.

The main achievements in the period covered by this report are related are described in the sections below.

User interface

In the third iteration, GUT was focused on the development of the user interface. At the moment, users can manage locations, gateways, reference nodes and beacons using the UI. The UI is now available both in English and Polish.

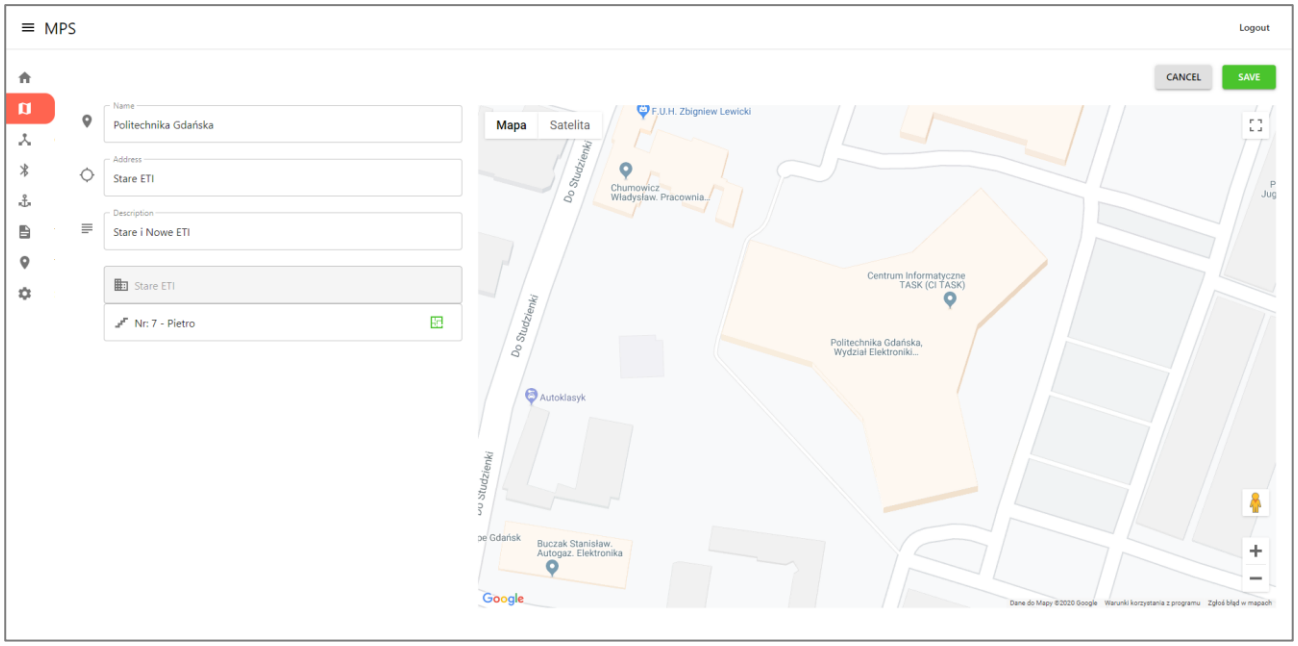

Figure 29: Adding a new location in the MPS UI

Device provisioning

In order to ensure easy deployment of the MPS, GUT developed a dedicated mobile app that can be used for deployment of the MPS Gateways.

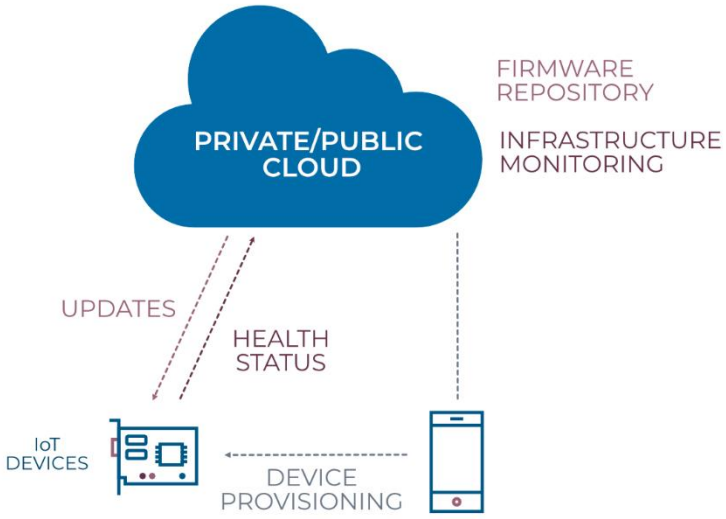

Figure 30: Device provisioning overview

Algorithms

In the third iteration, GUT was working not only on improvements of its main localization algorithm but also on a new one reducing number of required nodes.

Hardware

GUT ordered a variety of beacons that may be useful in the Emergency Department Equipment and Patient Tracking use case. Among them are beacons for tracking assets and people. The beacons have not been delivered yet. The test of the ordered beacons will take place in the upcoming months.

5 DISSEMINATION, EXPLOITATION AND STANDARDISATION

Refer to the corresponding section in D21.3 [5] for partner's ambitions and achievements concerning dissemination, exploitation and standardization. A brief update is given below.

5.1 Exploitation

Apart from the final demonstrator, Xetal is starting to commercialise the Yugen sensors and its related technology. Partners will be able to engage with Xetal to integrate the technology into their products (three such partnerships being finalised for 2020 already) or can engage with Xetal in order to use the sensors for internal building control (two such partnerships being finalised for 2020 already).

5.2 Dissemination

- Proposed publication by TU/e intended for the IJCAI-PRICAI2020, the 29th International Joint Conference on Artificial Intelligence and the 17th Pacific Rim International Conference on Artificial Intelligence. Title: *"Unsupervised sensory representation learning with scalogram contrastive network"* (Aaqib Saeed, Tanir Ozcelebi and Johan Lukkien). We developed a self-supervised learning approach for learning features from large unlabelled input in a federated learning context (i.e., learning on-device). Our methodology achieves competitive performance with fully-supervised networks, it works significantly better than pre-training with auto-encoders, and greatly improves recognition rate in a low-data regime.
- GUT visited the Emergency Department of one of the Copernicus' hospitals. GUT explained the possible improvements that MPS can bring and elicited the requirements.

Figure 31: The Head of the hospital presenting a plan of the building.

- Xetal will be submitting a scientific paper about the technology and, especially its use, to SPIE Photonics West 2021and will be demonstrating it commercially at CES 2021. While these events are taking place after the end of the project, we felt important to have a fully viable system and technology before engaging in any sort of scientific and commercial divulgation.

5.3 Standardization

No active contributions to standardization have been made in this 3rd iteration. Both PRE and Tellu have investigated and applied the use of FHIR standard based observation resources for monitoring devices in the healthcare domain.

6 INTEROPERABILITY

The message broker-based architecture of the ALCCS allows for easy integration with new functions as shown by the addition of the diabetes monitor and the SABAC. JSON based message formats have been widely used at interface level to allow for easy integration and simplified data exchange.

7 LINK TO TECHNOLOGY LINES

The table below summarizes the current status of the links between the ALCCS demonstrator and the SCOTT TBBs.

TBB	Core, Extended or Future?	Applicability and status of the TBB within WP21	TBB owner in WP21
BB23.O Security Core	Future	The BB23.O team has leveraged its expertise and methodology for secure system design to perform a security analysis on the ALCSS architecture and system developed by WP21. The analysis results in a device security classification and indicates where further security improvements may be needed.	PRE
BB23.P Spatial-based Authorization and Authentication	Core	GUT's Multimodal Positioning System (MPS) is re-used within WP21 as one of the sensory sources for indoor localization of persons. It is an integral part of the ALCSS architecture and has been fully integrated into the ALCCS demonstrator in this iteration.	GUT
BB24.G Mobile Edge Computing	Core	The Vemco edge node has a central role in the anticipated ALCSS system architecture to run all the (privacy-sensitive) processing related to the Resident's context. Security has been further improved based on a SCOTT security scan whitepaper.	VEMCO
BB24.I Semantic Attribute Based Access Control	Core	UiO's (S)ABAC technology has been identified to make contextual reasoning more dynamic and efficient, as explained in Section 3.3.6. This technology has been prepared for integration in the demonstrator.	UiO
BB24.L Adaptable Network Slicing	Extended	Mobile network slicing is expected to play an important role in enabling the "5G Connected Hospital". Isolation of two different network slices (one for ALCCS and one for healthcare) has been demonstrated, providing in parallel a robust and simple way of managing large-scale networking in cloud environments for mobile communication systems such as 5G.	Telenor
BB26.G Privacy Labels (A-F)	Extended	Privacy is a key concern for the Health Domain, in relation to sensitive patient data and consequently privacy or trust labels may offer value in this domain. UiO and PRE have worked together to see how to apply this in general and specifically for the ALCCS.	UiO

8 CONCLUSIONS

The ALCCS demonstrator from the 2nd iteration has been further improved w.r.t. privacy, security, and functionality:

- A privacy-preserving, distributed machine learning technique known as Federated Learning (FL) has been investigated for the ECD.
- Security of the cloud and edge interface has been improved by the addition of a vault (secrets manager).
- The multimodal positioning system (MPS) has been fixed and integrated into the ECD.
- SABAC to improve the scalability, dynamicity, security, and the precision of the access control mechanism has been evaluated and prepared for integration
- A Graphical interface for managing the Access Control System has been developed.
- The glucose monitor gateway App has been updated with authenticated session handling (based on OpenID connect) and support for a FHIR API.
- The 5G network slicing concept has been implemented and demonstrated using two isolated slices.

Another part of the work in the 3rd iteration focussed on the deployment of devices and technologies as applied in the ALCCS:

- The Xetal/Yugen thermal based presence sensor has been further improved to allow large-scale application
- Easy (LoRa) device to network commissioning to support large-scale deployment of IoT devices
- HL7/FHIR standard based device registration and observation reporting to support patient monitoring applications.
- Cellular (NB-IOT and CAT-M1) based connectivity of the ElderlyUI to support global device operation.
- Real Time Locating System (RTLS) technologies to support (indoor) localization for device (i.e. elderly/patient) tracking in emergency cases.

Furthermore a 2nd use case for localization of people and equipment has been evaluated and prepared. In a next iteration this may be deployed in the emergency department of a hospital.

9 REFERENCES

[1] SCOTT Deliverable D21.5, *"Use Case Specification and System Architecture for Assisted Living (iteration 3)"*, v1.0, 2019-06-28.

[2] SCOTT Deliverable D21.4, *"Applicability of Use Case and Building Blocks for Assisted Living Demonstrated (iteration 2)"*, v1.0, 2019-04-26.

[3] SCOTT Deliverable D21.1, *"Use Case Description"*, v1.1, November 27th, 2017-11-27.

[4] SCOTT Deliverable D21.2, *"Applicability of Use Case and Building Blocks for Assisted Living Demonstrated (Iteration 1)"*, v1.0, 2018-06-06.

[5] SCOTT Deliverable D21.3, *"Use Case Description"*, v1.0, 2018-08-23.

[6] SCOTT Deliverable D26.2, *"Reference architecture and reference implementations - Iteration 2"*, Version 1.0, 2019-03-10.

[7] Security Classification for Smart Grid Infra structures, Manish Shrestha, Christian Johansen, Josef Noll, UiO, Research Report 476, 2017: https://www.duo.uio.no/handle/10852/60948.

[8] Increase User Trust for a Bigger Market of Digital Technologies, SCOTT White Paper, Draft 1.4, January 2020.

[9] Saeed, Aaqib, Tanir Ozcelebi, and Johan Lukkien. "Multi-task Self-Supervised Learning for Human Activity Detection." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3.2 (2019): 61.

[10] ThinkPark Wireless Advanced Developer Guide V4, June 2017

[11] Fast Healthcare Interoperability Resources specification (R4): https://www.hl7.org/fhir

[12] ITU-T, HSTP-H812-FHIR - Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation, October 2019.

[13] GSMA eSIM Specification SGP.22 Version 2.2.1: https://www.gsma.com/esim/esim-specification.

[14] SCOTT Whitepaper, *"Security Scan Methodology for Cloud Connected IoT Devices"*, v1.0, September 2019.

[15] *LoRa Alliance Geolocation Whitepaper*, https://lora-alliance.org/resource-hub/lora-alliance-geolocation-whitepaper

[16] Positioning for the Internet of Things: A 3GPP perspective. *IEEE Communications Magazine, 55(12)*, 179-185.

[17] DecaWave Technology and Development kits: https://www.decawave.com/technology1/

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
3GPP	3rd Generation Partnership Project
5G	Fifth generation of cellular networks (upcoming generation of standards by 3GPP)
ABAC	Attribute Based Access Control
ACS	Access Control System
ALCCS	Assisted Living and Community Care System
AMQP	Advanced Message Queuing Protocol
BGP	Border Gateway Protocol
BioMKR	Smart watch product under development by Prediktor Medical, capable of CGM
BLE	Bluetooth Low Energy
Cat-M1	3GPP LPWAN standard for low-bandwidth communications (4.5G); higher bandwidth than NB-IoT
CGM	Continuous Glucose Monitoring
CI/CD	Continuous Integration and Continuous Deployment
CNI	Container Network Interface
CoAP	Constrained Application Protocol
ECD	Elderly Context Derivation
ESPAR	Electronically Steerable Parasitic Array Radiator
EU	European Union
FHIR	Fast Healthcare Interoperability Resources (see http://hl7.org/fhir/)
FL	Federal Learning
gNB	Next Generation Node B (3GPP base station for 5G)
IoT	Internet of Things
IoMT	Internet of Medical Things
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LoRa	Long Range (LPWAN standard)
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution (synonymous to 4G)
MME	Mobility Management Entities
MPS	Multimodal Positioning System
MQTT	Message Queueing Telemetry Transport
NB-IoT	Narrow Band IoT; 3GPP LPWAN standard for low-bandwidth communications (4.5G)
PIP	Policy Information Point
RTLS	Real Time Locating Systems
SABAC	Semantic Attribute Based Access Control (ABAC)

Term	Definition
TBB	Technical Building Block
TelluCloud	Cloud platform for creating products and services marketed by Tellu
UE	User Equipment
VoLTE	Voice over LTE
WDA	Wireless Data Aggregator