## SCOTT:

## Secure COnnected Trustable Things

# Use Case Specification and System Architecture for Assisted Living (Iteration 1)

| | |
|---|---|
| **Document Type** | Deliverable |
| **Document Number** | D21.1 |
| **Primary Author(s)** | Ewout Brandsma \| PRE |
| **Document Version / Status** | 1.1 \| Final |
| **Distribution Level** | CO (confidential – consortium only) |

---

| | |
|---|---|
| **Project Acronym** | SCOTT |
| **Project Title** | Secure Connected Trustable Things |
| **Project Website** | www.scottproject.eu |
| **Project Coordinator** | Werner Rom \| VIF \| werner.rom@v2c2.at |
| **JU Grant Agreement Number** | 737422 |
| **Date of latest version of Annex I against which the assessment will be made** | 2017-05-18 |

*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 |
|---|---|---|---|
| Ewout Brandsma | PRE | Lars Thomas Boye | TellU |
| Mateusz Mul | GUT / Vemco | Lukas Kulas | GUT |
| Peter Mörtl | VIF | Mateusz Rzymowski | GUT |
| Tanir Ozcelebi | TU/e | Christian Johansen | UiO |
| Aaqib Saeed | TU/e | Toktam Ramezanifarkhani | UiO |
| Francesco Pessolano | Xetal | | |

# FORMAL REVIEWERS

| Name | Organization | Date |
|---|---|---|
| Łukasz Szczygielski | GUT | 2017-11-24 |
| Claudio Henrique de Castro | Embraer | 2017-11-26 |

# DOCUMENT HISTORY

| Revision | Date | Author / Organization | Description |
|---|---|---|---|
| 0.1 | 2017-10-12 | Ewout Brandsma / PRE | Baseline version by copying scenario description diagrams of Mateusz Mul and end-to-end description of Peter Mörtl into the new UC description template |
| 0.2 | 2017-10-16 | Ewout Brandsma / PRE | Adding content for Section 3.1 |
| 0.3 | 2017-10-23 | Ewout Brandsma / PRE | Initial edits following discussion during Porto F2F |
| 0.5 | 2017-10-30 | Ewout Brandsma / PRE<br>Mateusz Mul / GUT/Vemco, Tanir Ozcelebi / TU/e | Restructuring/reviewing use case scenarios and aligning with end-to-end scenario. Added architecture overview. |
| 0.6 | 2017-11-02 | Ewout Brandsma / PRE | Updated Section 3 following 31/10 conference call. In particular refined role of voice call and removed Call Center as an explicit actor (now just another Caregiver). |
| 0.7 | 2017-11-07 | Ewout Brandsma / PRE | Added Sections 1, 2, 4.1, 5, 6, 7 and Appendix A (i.e. complete except for 4.2). |

| Revision | Date | Author / Organization | Description |
|---|---|---|---|
| 0.8 | 2017-11-13 | Ewout Brandsma / PRE<br>Lukasz Kulas / GUT<br>Lars Thomas Boye / TellU<br>Mateusz Mul / GUT | Added dissemination and exploitation (Section 4.2). Added TellU use case (Appendix B). Updated UML system diagram to align with updated scenario descriptions. Elevated document to "Proposal" level. |
| 0.9 | 2017-11-14 | Toktam Ramezanifarkhani / UiO<br>Christian Johansen / UiO<br>Ewout Brandsma / PRE<br>Mateusz Mul / GUT/Vemco<br>Lukasz Kulas / GUT | Added UiO, Xetal and PRE dissemination activities and some further updates to dissemination. Textual fixes and updates of related building blocks and requirements. Reviewed in WP21 telco without further comments. |
| 1.0 | 2017-11-24 | Ewout Brandsma / PRE | Processed comments of formal review by Damian Duraj (GUT) and Łukasz Szczygielski (GUT). Elevated document to "Approved" level. |
| 1.1 | 2017-11-27 | Ewout Brandsma / PRE<br>Lars Thomas Boye / TellU | Processed comments of formal review by Claudio Henrique de Castro (Embraer). Renamed "Approved" into "Final". |

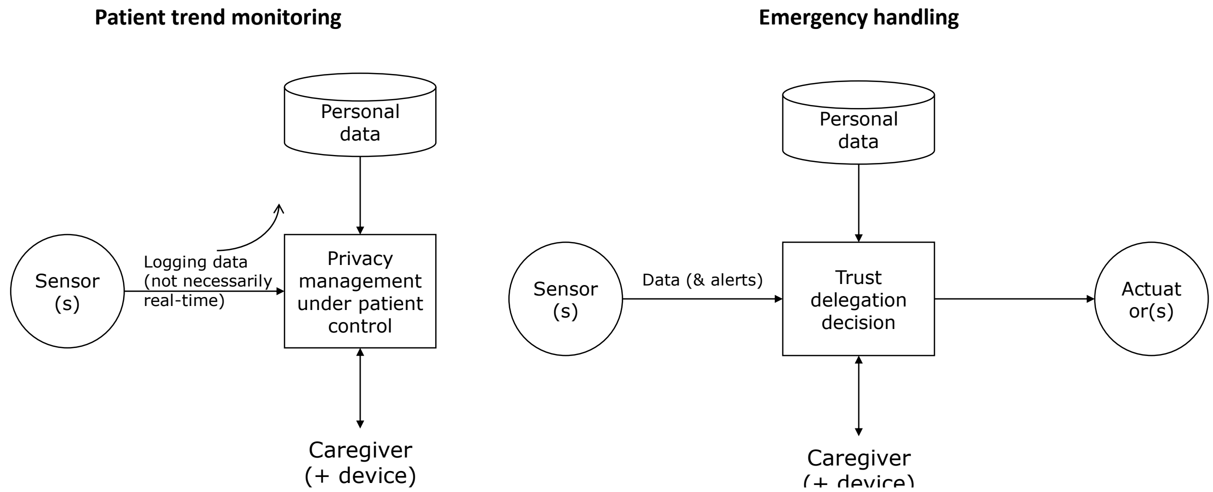
# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

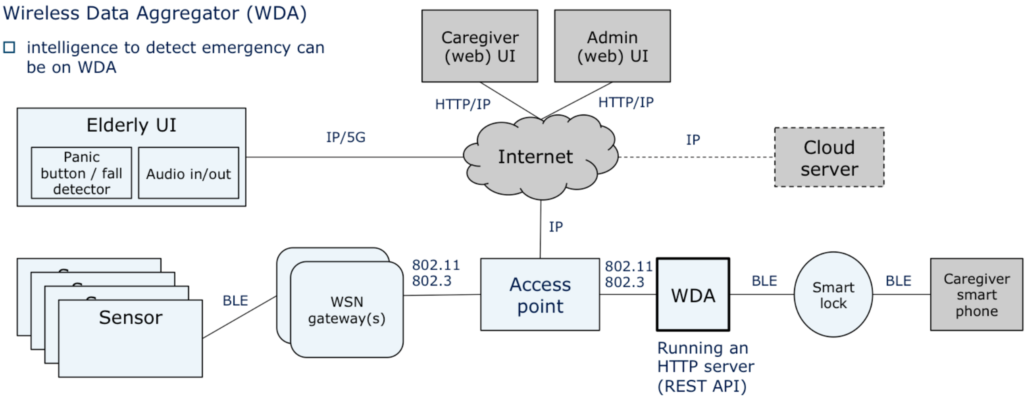
# 1 EXECUTIVE SUMMARY

An iterative approach towards exploring trust delegation in the healthcare domain is proposed addressing the ‘template’ use cases ‘patient trend monitoring’ and ‘emergency handling’. Trust delegation enables a patient or individual at risk to determine who can access what (medical data, access to home, etc) under which circumstances, all in a very trustful, transparent and intuitive manner.



For the first iteration – aiming at a first demonstrator in M14 – a specific use case in assisted living and community care is worked out in more detail. It enables frail elderly people – who are e.g. prone to falling – to remain living in the comfort of their own home longer, in an attempt to curb the ever soaring costs of healthcare and an aging population. The solution involves a personal emergency response system using multi-modal sensoric information to infer the context of the elderly resident, as well as that of potential caregivers, to determine the most appropriate caregiver to help. In many cases, this could be an informal caregiver enabling less costly – and more trustful – exploitation of the personal emergency response system. The most critical scenarios are worked out in detail with activity diagrams and a first multi-view architecture is sketched.

Avoiding costly intervention of a centralized call center, unless absolutely necessary, and processing all privacy sensitive data through on-premise edge computing constitute the major progress beyond the state-of-the-art.



**Keywords:** trust delegation, patient trend monitoring, emergency handling, personal emergency response systems, context derivation, localization, direct-to-cloud, cellular IoT, healthcare, IoMT, 5G.

# 2 OBJECTIVES

## 2.1 Deliverable objectives

The objectives of the current deliverable are:

- Present the context of the use case ”Assisted Living And Community Care” as being a first example (i.e. iteration) use case to explore the applicability of ‘trust delegation’ for connected systems in healthcare (Section 3.1).
- Present the SCOTT Trust Framework mapping for this use case by means of an end-to-end scenario description (Section 3.3).
- Present detailed functional scenarios for this use case, linking SCOTT TBB’s and their associated requirements where applicable (Section 3.4 and 6).
- Present a first iteration of the High Level Architecture of components for realization of the use case (Section 3.2).
- Provide a description of actions related to dissemination, exploitation and standardisation (Section 4).
- Identify interoperability related topics for this use case (Section 5).

## 2.2 Work package objectives

The objectives of WP21 are [1]:

- Provide solution for secure **trust-based delegation** in assisted living and community care. This involves the actual delegation, how this is modelled and executed using some protocol on the one hand and the trust computation plus context evaluation that underpins the decisions on the other hand.
- Provide solution for automated **context derivation for resident as well as potential responders**. This involves wirelessly connected sensors monitoring the resident’s home, as well as his/her vital signs to assess personal health, wellbeing and trustable system operation. It also involves reliable and secure geolocation (enables spatial-based authentication) to help finding the most appropriate responder.
- **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. For the latter, stakeholder (e.g. focus group), as well as social science involvement is needed throughout the process to continuously improve the demonstrator with the end-user in mind.

The first iteration use case outlined in the current deliverable specifies such a demonstrator that infers Resident and Caregivers‘ (i.e. responders‘) contexts based on sensory data and location to compile a list of eligible Caregivers and delegates access to the Residents home through a SmartLock. It should be noted that future iterations may explore trust-based delegation in a broader healthcare context than just elderly care.

## 2.3 Link to overall SCOTT objectives

The SCOTT general objectives [1] and the way they are addressed in WP 21 are described below.

### 2.3.1 Focus on wireless systems

As can be seen from Figure 4, the envisaged demonstrator utilizes in-home wireless connectivity technologies such as Wi-Fi, BLE and proprietary ones, not just to communicate, but also to localize and to securely enter a building through proximity. However, WP21 will move beyond those well-established technologies and explore novel low-power, low-bandwidth, low-cost, high-coverage cellular technologies such NB-IoT and Cat-M1 for enabling affordable, reliable, anytime, anywhere connectivity to the device worn by the Resident. Those technologies, in turn, will be a pre-amble to a much wider palette of cellular technologies for IoT that will be offered by the upcoming fifth generation of mobile networks (5G). One of those 5G technologies considered in WP21 is Network Slicing as addressed by the linked TBB BB24.L. While 5G will obviously not be part of the first iteration demonstrator described in the current deliverable, our thinking for future iterations will be guided by those possibilities.

### 2.3.2 Focus on European leadership and market opportunities

Connected healthcare propositions address one of the most pressing European (and global!) Societal Challenges, namely the one on health and wellbeing. Specifically, the solution proposed in the current deliverable enables frail elderly to remain living in the comfort of their own home longer, thus improving their wellbeing and at the same time providing an answer to the soaring costs of healthcare (currently around 10% of GDP across most of Europe). More in general, the ability of connected healthcare propositions (powered by 5G or otherwise) to allow frail individuals and patients to remain in lower-cost care settings will enable a substantial savings in healthcare expenditure and that obviously enables plentiful market opportunities for the European industry.

### 2.3.3 Focus on smart sensor and actuators

The envisaged demonstrator comprises a Smart Lock as a first example of a smart actuator and a variety of state-of-the-art sensors, most notable to be able to localize elderly persons in their own home, as first examples of smart sensors. For future iterations, various wearable vital-sign sensors, as well as ubiquitous localization can be considered.

### 2.3.4 Focus on Security, Safety, Privacy and Trustability

The edge-based trust-delegation solution described in the current deliverable enables an elderly person to automatically solicit help from familiar Caregivers, such as family members in a very privacy-aware manner. Specifically, the on-premise Edge System takes care of all context derivation and trust-based delegation, so any information about ‘accidents‘ and people involved does not have to leave the house, unless the urgency of the accident requires so (e.g. calling 112).

Observe that the use case described in the current deliverable will focus on edge computing mode (distributed), as opposed to cloud computing mode (centralized), although the option to offload some processing to the cloud, i.e. mixed computing mode is kept open. These three concepts are defined in [1] as follows:

- **Cloud computing mode (centralized)** – where context reasoning rules (related to the detection of emergency situations inside the home) are implemented in the cloud as specialized services – it involves transferring of sensitive data outside the home bubble, but eliminates the necessity of implementing sophisticated reasoning engines in the home infrastructure.
- **Edge computing mode (distributed)** – where context reasoning rules (related to the detection of emergency situations inside the home) are implemented in the WDA (the cloud will only share

the actual service repository, which will be distributed to home infrastructure) – it eliminates the problem of transferring sensitive data outside the home bubble, but causes the necessity of ensuring local services and infrastructure with required computational power.

- **Mixed computing mode** – depending on the processed data type (e.g. the level of their confidentiality, sensitivity), the available infrastructure trustfulness level (established on the basis of e.g. Privacy Labels t.b.d.), power supply mode of system components (battery or mains – for optimal energy management) – in short: optimization of balanced data processing and distribution.

### 2.3.5 Focus on including psychological and socio-contextual enablers for trust formation

The end-to-end operational scenario described in Section 3.3 forms the first step of the SCOTT Trust Framework, where socio-contextual issues are considered to address trust formation. Specifically, considering this end-to-end description, surfaced the importance of human contact in trust formation, which is the reason that the Caregiver will attempt to set up a voice call before deciding to head over to the elderly's home.

### 2.3.6 Focus on eco-system with well-defined re-usable Technical Building Blocks

As described in Section 3.1 (Table 1) and Section 6, WP21 intends to re-use TBB's BB23.O, BB23.P, BB24.G, BB24.I and BB24.L. Focus of the first iteration use case description of the current deliverable is on BB23.P (”Spatial-based authorization and authentication“), BB24.G ("Mobile Edge Computing“) and BB24.I (“Semantic Attribute Based Access Control”).

### 2.3.7 Focus on solutions to be used in multiple industrial domains

Connected healthcare propositions, such as the one around assisted living and community care pursued in the current deliverable, have an obvious link to the building and home domain (e.g. the use of a connected door lock to allow authorized Caregivers to enter the home of an elderly person). The same TBB's BB23.P, BB24.G and BB24.I are also used in use cases from that domain.

### 2.3.8 Focus on higher Technology Readiness Levels (TRLs)

Although WP21 takes an explorative approach to further shape the concepts around trust delegation (i.e. TRL 5), some of the linked TBB's and partners may have an ambition at levels 6 and 7.

# 3 DESCRIPTION OF WORK

## 3.1 Context of the Use Case

Trust and trustworthiness are the basis for taking decisions, certainly in a care setting involving vulnerable individuals. Within the scope of healthcare, decisions entail, for example, sharing – often sensitive – personal data, providing access to devices or premises and contacting care professionals or family members. In case these decisions need to be taken – or at least supported – automatically by electronic devices, a basis of trust needs to be established electronically, as part of the system operation. This is known as 'trust delegation'.

The main innovation of WP21 will be the development of solutions addressing trust delegation. This will be done in an iterative manner. A total of three iterations is planned throughout the course of SCOTT. Different use cases throughout the healthcare continuum may be prototyped in these successive iterations. Each use case will have specific requirements for trust delegation, for example in terms of the data or the physical assets (devices, premises) to be accessed.

Two distinct 'template use cases' can be distinguished: patient trend monitoring (see Figure 1) and emergency handling (see Figure 2). Any concrete use case to be prototyped will be an instantiation of one – or both – of these template use cases.

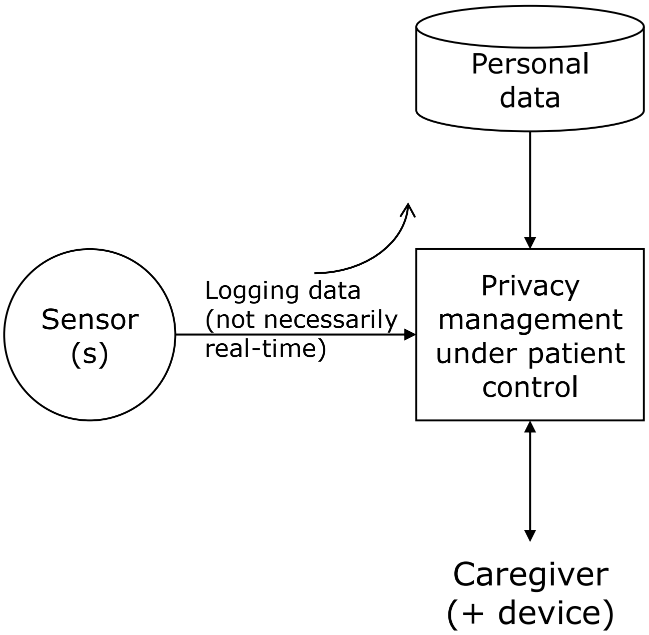

Personal data
Logging data (not necessarily real-time)
Sensor (s)
Privacy management under patient control
Caregiver (+ device)

**Figure 1 Trust delegation for patient trend monitoring**

Patient trend monitoring is about monitoring a patient's vital signs (often continuously) to support diagnosis and report early signs of deterioration. For example, a heart patient experiencing arrhythmias could be monitored continuously to assess the frequency and severity of the arrhythmias and a treatment plan could be made accordingly. This is part of a trend where more-and-more patient data is collected (linked to the trend on quantified self), which implies that privacy will be a growing concern. For this reason it is imperative that the patient must be in control of his own data. In this case trust delegation means that the patient can determine who can access what part of his medical data under which circumstances, all in a very transparent and intuitive manner.

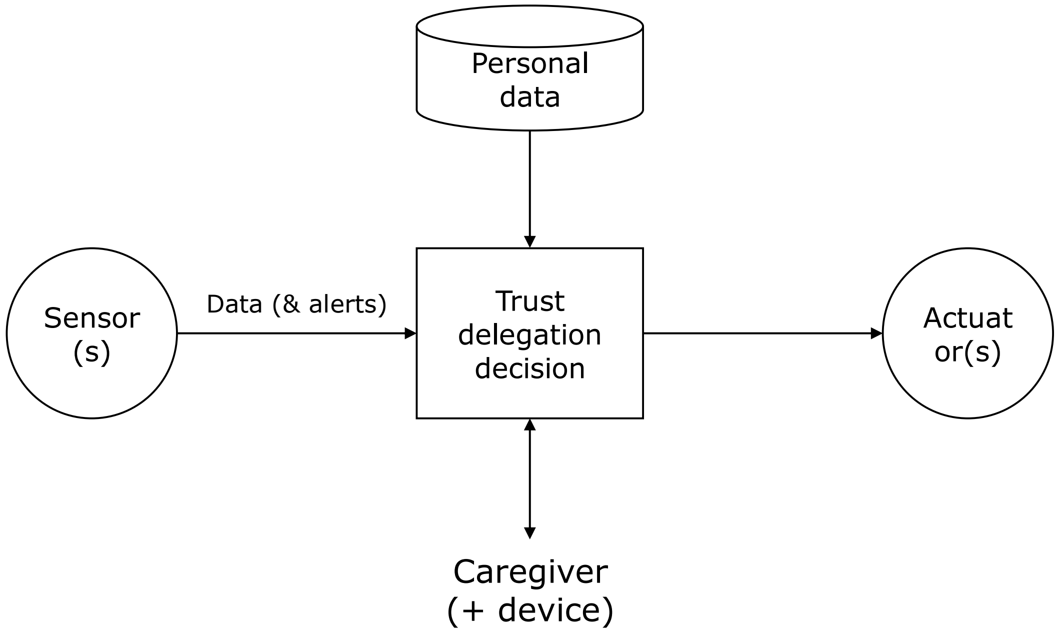


**Figure 2 Trust delegation for emergency handling**

Emergency handling is about arranging the quickest and most appropriate care when a patient experiences an emergency. For example, an elderly person living alone, possibly suffering from mild dementia, may have fallen and not be able to get up again or be incapacitated in another way. Such a situation could be detected, for example, by using a panic button, a fall detector or by tracking the person's location and movements. In this case trust delegation involves locating the most appropriate person in the vicinity to give immediate care and providing him or her with access to the elderly's home (wirelessly controlled lock on the front door) as well as relevant medical data about the individual. Another example involves emergency care in case of Sudden Cardiac Arrest (SCA), where a large network of qualified layman responders could be leveraged to provide care (CPR, AED) to a nearby patients experiencing SCA. In case such an emergency is detected, these layman responders will be provided access to otherwise closed buildings to pick up an AED. As can be seen, emergency handling involves access control, not only to patient data, but also to physical assets (devices, premises). The latter means that the system will also include actuators (e.g. wirelessly controlled locks).

The remainder of the current section (i.e. Sub-sections 3.2, 3.3 and 3.4) describes the requirements for a minimal viable product; a personal emergency response system (and service) that provides an example of trust delegation for emergency handling in case an elderly person has an accident in his or her own home. A novel aspect of this solution is that the most appropriate Caregiver is selected based on the actual context of the Resident, wheras present-day solutions patch the Resident through to a centralized call center. In most cases, contacting a nearby informal Caregiver (e.g. next-of-kin) may suffice, avoiding costly responses by professional Caregivers. It is, for example, known that elderly sometimes push the alert button just to have some human contact. In the Netherlands recently it appeared in the news that elderly who push the alert button more than a few times per year get charged significant costs in addition to their regular subscription fee [2]. This news led to public outrage, including questions in parliament.

Avoiding costly intervention of a centralized call center, unless absolutely necessary, and processing all privacy sensitive data through on-premise edge computing (as outlined in Section 3.2.1) constitute the major progress beyond the state-of-the-art.

Another use case combining elements of patient trend monitoring and emergency handling will be pursued by **TellU** addressing the needs of children with diabetes. This use case is briefly sketched in Appendix B and will be worked out in more detail in forthcoming deliverables. It will provide another example of applying trust delegation by leveraging the S-ABAC building block BB24.I.

Note, that the M14 demonstrator (D21.2) may only implement part of the features and aspects stated in the current deliverable depending on effort and lead time available.

Table 1 provides an overview of the TBB's linked to this use case. The implementation for this first iteration will mostly focus on BB23.P, BB24.I and BB24.G. The Security Core (BB23.O) may possibly be covered indirectly through those TBB's and not directly through the current use case, whereas BB24.L is likely to be covered by later iteration use cases that have more demand for privacy aware and/or guaranteed delivery to centralized cloud components.

| ID | TBB | COMPONENTS | OWNER |
|---|---|---|---|
| 1 | BB23.O Security Core | Will use the recommendations of this TBB when choosing technical solutions for data protection at rest and in transit (i.e. encryption) as well as to enable proper authentication and authorization. Much of this may happen through other TBB's (23.P, 24.I). | PRE |
| 2 | BB23.P Spatial-based authorization and authentication | VEMCO – SW modules allowing for additional authorization of user / object through usage of information about current position in building. GUT – SW + HW allowing for object localization – Multimodal Positioning System (MPS). | GUT |
| 3 | BB24.G Mobile Edge Computing | Implementation of sub-clouds, placed in device work environment, used for data management that requires short time response. Visualization module for processing node (or resource usage) and response time. Implementation of two different modes: centralized processing and edge computing. Management of access distribution process. | VEMCO |
| 4 | BB24.I Semantic Attribute Based Access Control | Access control system based on existing open source engines, or extensions of these with custom fit solution tailored to the technological innovations done in this BB. Access control policies defined based on the Scenarios described in the WP21. Semantic modules including ontologies and reasoning engines, integrated with the access control engine and policies. | UiO |
| 5 | BB24.L Adaptable Network Slicing | Lab-scale testbed enabling 5G network slicing on LTE network. | Telenor |

**Table 1 TBBs and Components**

## 3.2 High Level Architecture of the Use Case Components

The SCOTT solution specification will include a reference architecture that introduces relevant concepts and their relationships presented as a multi-view model (see Figure 3) supporting an exploration of design decisions, modeling of stakeholder concerns at a generic level.

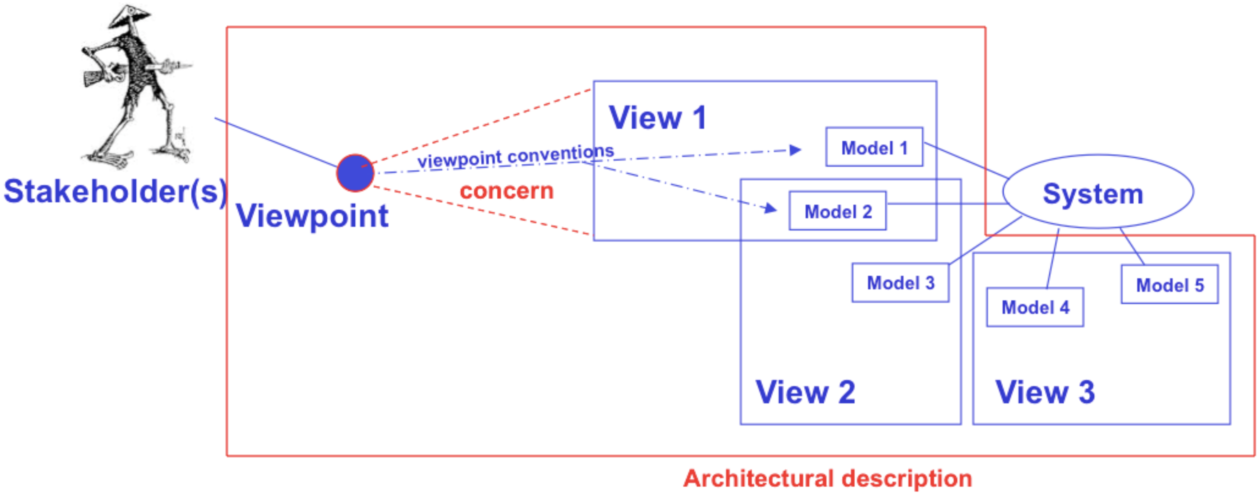


**Figure 3 Multi-view model**

The goal of this section is to describe a concrete high level architecture of the use case implementation under consideration. This is meant to be an instantiation of the reference architecture, filling in design decisions, with a given structure of nodes, logical components and networks, and the corresponding activities.

### 3.2.1 Physical View

The physical view shows the physical topology of the (networked) system, as well as the connections between different components as given by Figure 4. It is typically accompanied with what is called a deployment view, describing the deployment of logical components on physical devices in the topology as shown in Figure 5.

The system will comprise different sensor types, both worn as well as deployed throughout the home. The Elderly UI, provided by **PRE**, is a device worn by the Resident comprising a panic button and optionally a fall detector and/or various vital-sign sensors. The Multimodal Positioning System (MPS), provided by **GUT/Vemco**, includes the use of worn BLE beacons whose location is determined by means of one or more WSN gateways. **Xetal** provides a system that is able to track individuals throughout the home without the need for any wearable. It comprises fixed IR temperature sensors deployed throughout the home and (another type of) WSN gateways to collect their data.

Notice that the Cloud server is an optional extension of the WDA (Edge System), which may be used to offload it for more demanding computations.

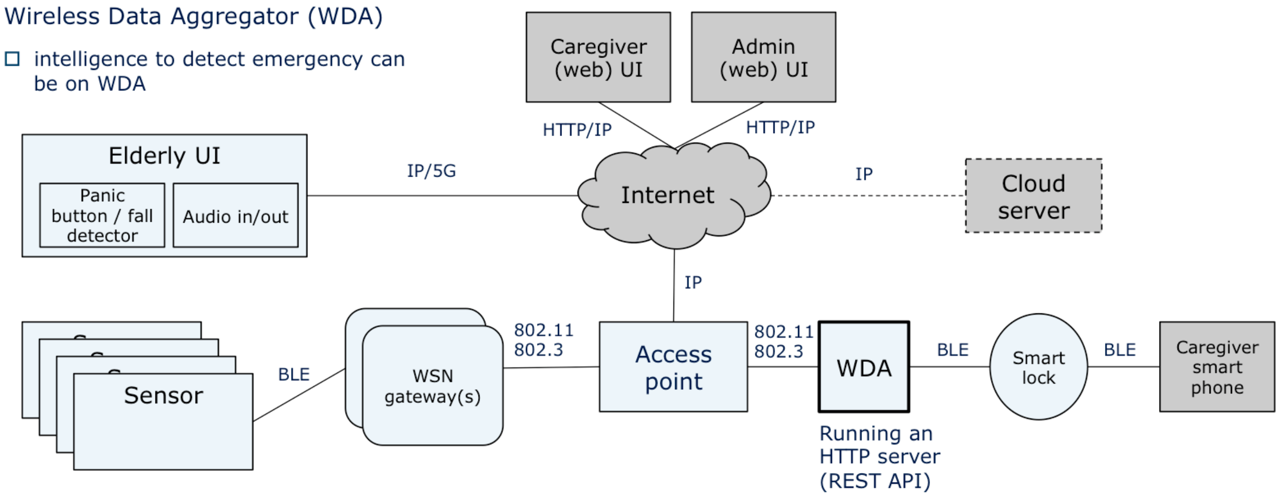


**Figure 4 Physical view: physical topology of the system**

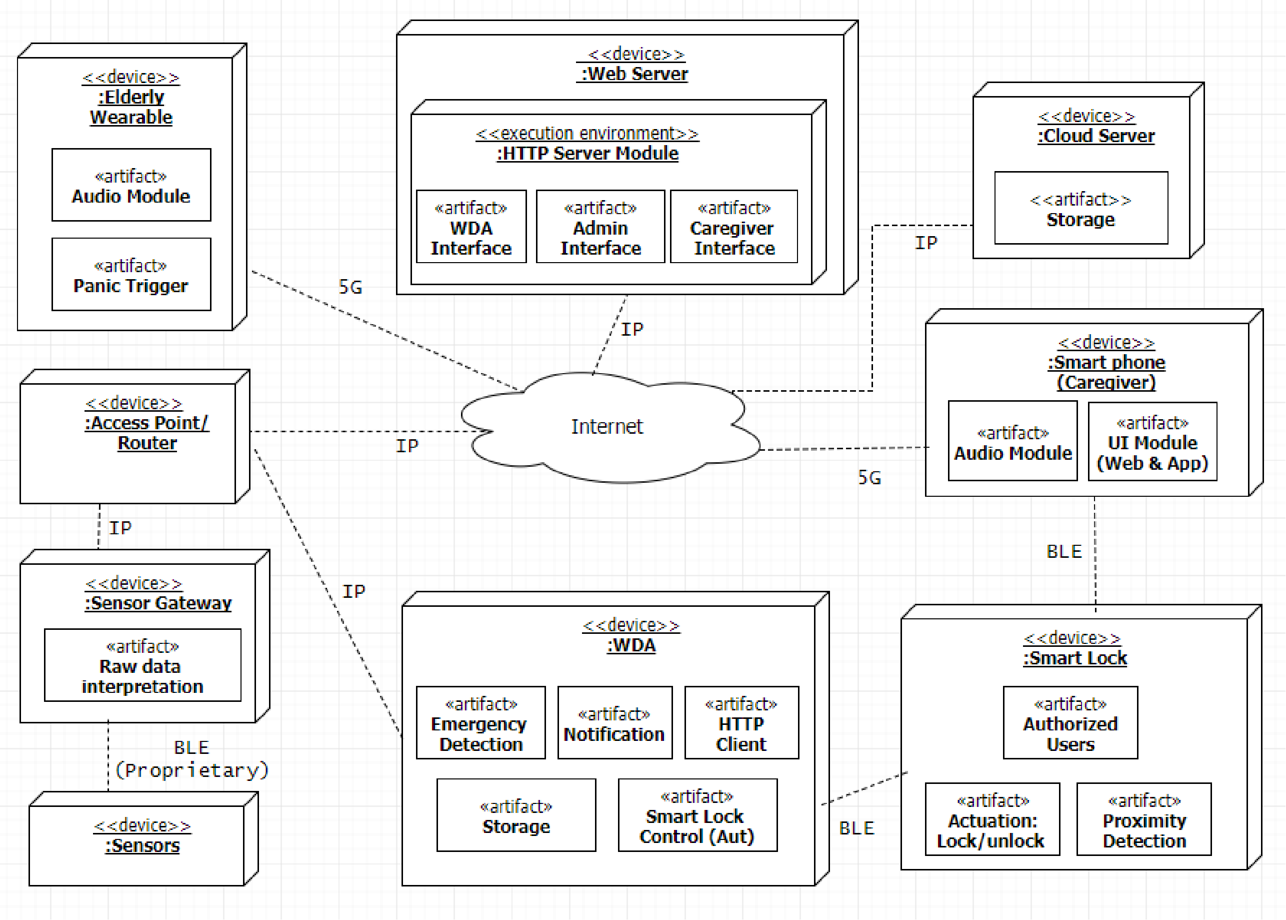


**Figure 5 Physical view: Deployment of logical components**

## 3.2.2 Logical View

This view concerns the functionality of the system. That is, it describes the logical components, their properties, their functions and the interrelations between them. The logical view for the emergency detection use case implementation is shown in Figure 6 below.

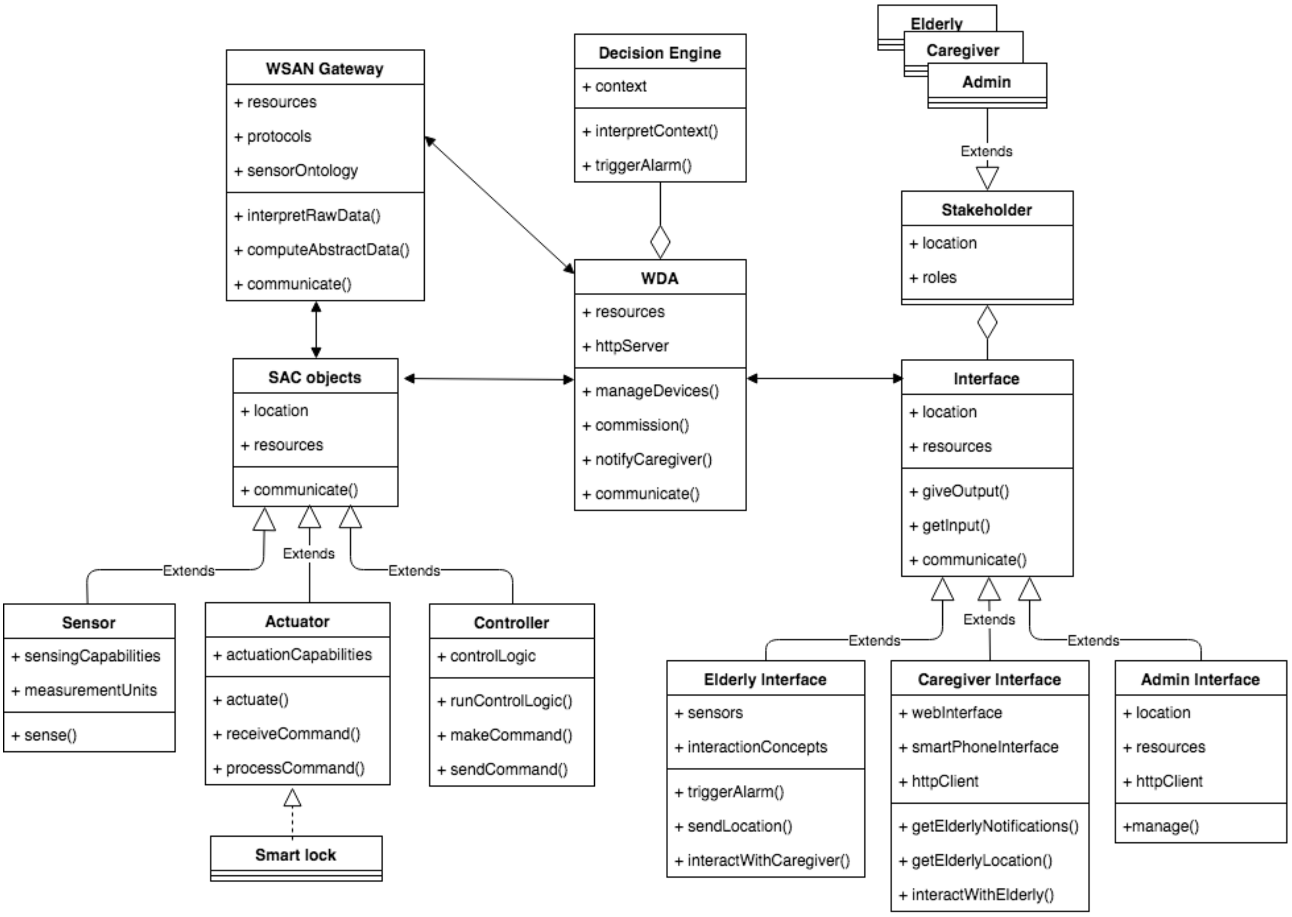


**Figure 6 Logical view**

## 3.2.3 Development View

The development view describes the software implementation typically in a package diagram showing the dependencies between various software components as shown in Figure 7.

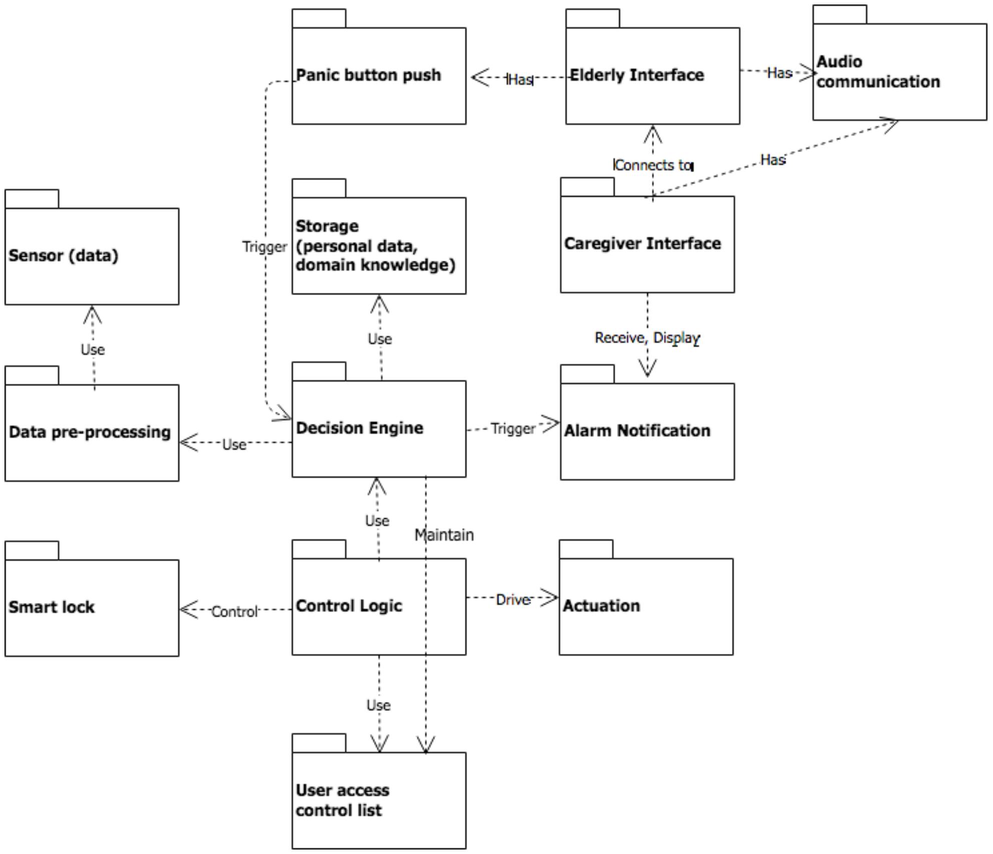


**Figure 7 Development view**

### 3.2.4 Scenarios and Process View

The scenarios of interest and the corresponding process view (in the form of activity diagrams) are given in Sections 3.4.

## 3.3 End-to-End Operational Scenario

In order to (1) assess, (2) facilitate, and (3) assure trustability of SCOTT use cases, a detailed operational description of the end-to-end system usage describes what the system does, who uses it, how, and under what conditions. The end-to-end operational scenario motivates and provides the main requirements for the more specific technical use cases that are described in later sections of this document. Because SCOTT is developed in an agile manner, in the early phases of the process, the end-to-end operational scenarios and the technical use cases may not yet be completely aligned. However, over the course of the project they will converge in the end. The end-to-end operational scenarios provide the basis to derive trust requirements and to assure trust worthiness at the end of the SCOTT project. For use cases for which no end-to-end operational scenarios can be identified, this section remains empty and an explanation is provided for why that is the case. The figure below shows the linkage between end-to-end operational scenarios, technical use cases, and the overall development of a trusted system:

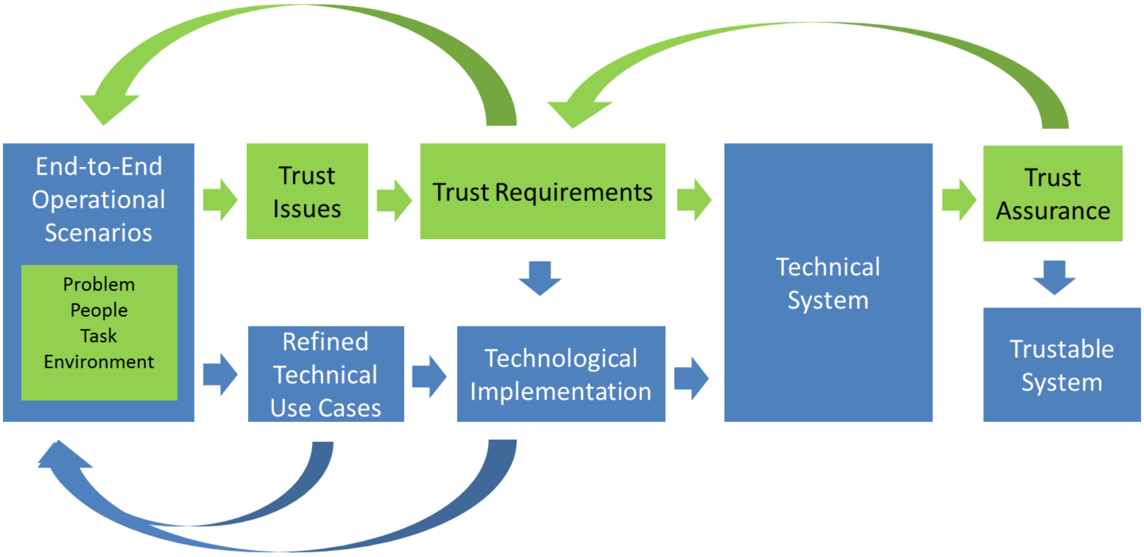


**Figure 8 Relation between End-to-End Operational Scenario and refined technical use cases**

The end-to-end operational scenario describes as concrete as possible the problem and the innovative solution in terms of the people, their tasks, and their environment. The technical implementation is not the focus, in fact, the operational scenario should precede the technical approach and help motivate it. While many possible operational scenarios exist, only a single one that is representative for many is described in this section. The other descriptions would follow this template.

### 3.3.1 Objective

The purpose of the Assisted Living and Community Care System (ALCCS) system is to detect severe anomalies in the sensed data and, if needed, initiate an emergency response, as well as enable better diagnostic decisions by the medical doctor.

- The problem situation: An elderly resident wants to live at home but his family is concerned about him or her falling and not being able to get help.
- The current solution: Currently available systems require the resident to wear an emergency unit (such as a pendant around the neck or a bracelet/watch worn around the wrist) and press a

button that then calls the emergency responders. Also neck-worn devices exist that support automated fall detection. The resident may forget to wear the emergency response unit. The emergency team may not have access to the home and has no information about the resident's condition.

- The basic innovation: The emergency unit consists of a wireless sensor that is worn directly on the skin (i.e. non-detacheable) and automatically detects a resident's fall along with critical body sensor information that helps the system to quickly plan the appropriate response[1]. Also, the system provides appointed caregivers (i.e. responders) quick access to the resident's home.

### 3.3.2 Operational Scenario

Jeff is 80 years old and his daughter Jennifer has recently observed that he is less stable on his feet than he used to be. Jeff lives alone but is frequently visited by his daughter. When talking about this to Jeff's general practitioner, Jennifer learns about the Assisted Living and Community Care System (ALCSS), an advanced form of fall detection and alerting system. In contrast to similar systems, ALCSS does not only allow to automatically detect a resident's fall without the resident having to wear an external device (existing products require a sensor to be worn around the neck or the arm), but it also gives caregivers access to an elderly's home to allow swift and easy access. The ALCSS consists of a sensor that is very small and is directly worn on a person's skin and able to reliably detect falls and shows absolutely no skin irritations.

The next day, Jennifer calls the ALCSS provider for more information. They schedule a visit of their sales agent, John. John visits Jennifer and Jeff the following day. John informs them about the product and also assesses Jeff's situation to determine how the ALCSS could be adapted into Jeff's environment: Jeff lives alone in his house in the suburbs of a major city, about 30 minutes away from his daughter Jennifer who is closest to Jeff. His wife has passed away last year. John informs Jeff that in order to ensure to get emergency help after a fall, the ALCSS must need to give appointed caregivers (e.g. Jennifer, a neighbor or an ambulance crew) access through the main door of Jeff's house. Therefore the lock would have to be replaced with one that can be opened via a wireless ALCSS device by the appointed caregivers. Jeff is at first uncomfortable about giving somebody else access to his home. John responds that the ALCSS can be paired with an integrated home security system that not only increases protection agains burglars but also provides personalized security for the whole house (e.g. includes windows and other side-entrances)[2]. The system that would be alerted after an automatically detected fall also handles 24-7 security services. Only once the system has indicated that Jeff may have a medical emergency, it becomes possible for the responding caregiver to enter Jeff's house with an ALCSS door opener, so that Jeff doesn't have to open the door.

Jennifer sees that Jeff is convinced and supports Jeff signing up for a 3 month trial. John installs the base unit of the ALCSS health monitoring system and goes with Jeff through a standard form to assess who should and should not have access to the house. Jeff decides that Jennifer, his Doctor,

[1] A skin-worn device that senses critical vital sign data, as well as falling is just one of many possible modalities to detect an anomaly. The use case scenarios described in Section 3.4 describe a panic button and detecting anomalies in location or vital signs. Fall detection is existing technology and functionally equivalent to a panic button. It is however hard to realize in a trustful way when worn around the wrist (because rapid arm movements are hard to distinguish from falling down).

[2] The integrated home security system is not described as part of the use case scenarios in Section 3.4, as such systems are commonly known and a detailed description of such a scenario and its realization in a SCOTT demonstrator is therefore considered neither innovative nor valuable, in spite of such functionality possibly instilling end-user trust in an eventual market offering.

and official emergency responders (e.g. ambulance service) can get access to the house. John informs Jeff that only he can change these settings by contacting the ALCSS help desk. In addition, John tells Jeff that the ALCSS help desk can determine that only Jeff will be able to change any of the settings using a build-in voice recognition system that is able to automatically identify Jeff[3]. Nobody else will be able to change any of the settings. Jeff trusts John who is polite, knowledgable and effective. This positively impacts Jeff's trust formation toward the ALCSS. They take a voice sample to set up the automatic voice recognition. Jeff will not have to remember any password, pin, or anything.

The next day, the ALCSS installation crew arrives and installs the necessary sensors, locks, and actuators. Also, Jennifer receives an ALCSS emergency door opener via mail, and both Jeff's Doctor, and the official emergency responders are registered as authorized to open Jeff's front door in case of an emergency.

One month later, Jeff is just brushing his teeth in the evening when he moves quickly and slips and falls on the bathroom floor. He is not able to move and the ALCSS detects the fall, because it knows that Jennifer is out-of-town and cannot respond quickly enough, the ALCSS sends a signal directly to the 112 call center and the on-duty dispatcher calls Jeff on his wearable. Jeff hears the voice from the wearable, but is not able to respond loud enough to be audible by the dispatcher.  Because the dispatcher does not receive a response from Jeff, he sends an ambulance. Bob, the emergency responder in charge has just recently received his ALCSS door opener that is personalized to him. The ALCSS system knows who opens what doors, and when, and logs all this information for later cross-checking to minimize misuse. When Bob arrives with his crew at Jeff's house, they use the ALCSS door opener and find Jeff in the bathroom. Upon finding him, the dispatcher gets a message and Jeff's daughter Jennifer is informed that Jeff has likely broken his hip so that she can immediately come to the hospital.

[3] Although changing access settings in a trustful and user-friendly manner (especially considering the specific vulnerabilities of the target group) is key to instilling end-user trust, it is not considered a key topic for SCOTT innovation and therefore not covered by a use case scenario in Section 3.4. The SCOTT demonstrator may utilize different means than voice recognition to authenticate Jeff.

## 3.4 Use Case Scenarios

The Use Case Scenarios presented in this section are built around key functionalities of the described environment. A scenario describes one of many possible utilizations of components implemented in the Work Package. The description of WP21 from functional perspective is presented here. UML use case diagrams are used to provide a big picture of the functionalities proposed.

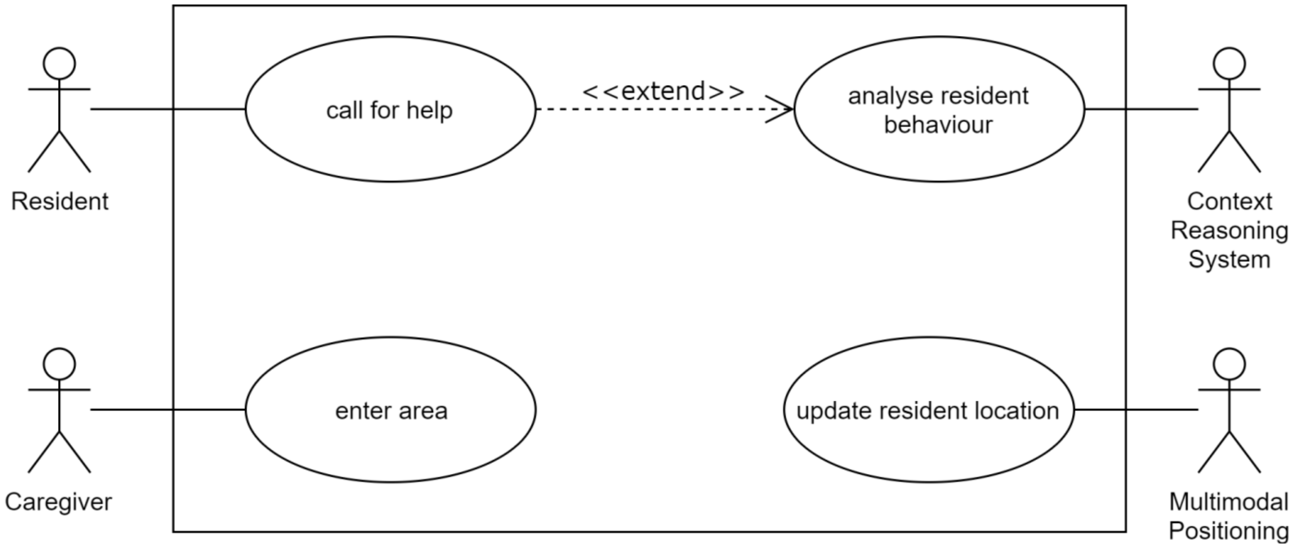


**Figure 9 Assisted Living and Community Care use case**

### 3.4.1 Scenario 1: Call For Help

| | |
|---|---|
| **Use Case** | WP21 Assisted Living and Community Care |
| **Scenario** | Call For Help |
| **Actors** | Resident – wants to get help from the most appropriate trusted person in case of an emergency.<br>Caregiver – wants to get information about the emergency and access to the facilities to be able to resolve it. |
| **Description** | This scenario describes a procedure of calling and dispatching the most appropriate Caregiver for help in case of an emergency situation. |
| **Trigger** | The Context Reasoning System triggers the Call For Help (note: a panic button push by the Resident is handled through the Context Reasoning System as well). The Context Reasoning System has prepared a prioritized list of Caregivers based on the contexts of Resident and potential Caregivers. |
| **Normal flow of events** | 1. The Edge System receives a Call For Help from the Context Reasoning System, retrieves the prioritized list of Caregivers and sends an emergency signal to the most appropriate Caregiver (i.e. top of the list).<br>2. The selected Caregiver receives the emergency signal, decides to accept the call and to initiate a voice connection with the Resident.<br>3. The Resident doesn't respond or the Resident responds and indicates he/she is in an emergency situation (or setting up the voice call fails).<br>4. The Caregiver indicates whether he/she can handle the emergency himself/herself:<br>a. If the Caregiver can handle the emergency: subscenario S-1 is performed.<br>b. Else: S-2 is performed. |
| **Sub flows** | S-1. The selected Caregiver can handle the emergency:<br>a. The Edge System sends credentials of the responding Caregiver to the SmartLock of the frontdoor of the Resident's house.<br>b. The SmartLock updates the access credentials with the ones from the responding Caregiver.<br>S-2. The selected Caregiver can't handle the emergency:<br>a. The Caregiver provides additional context information based on his/her voice call conducted with the Resident.<br>b. The Analyse Behaviour scenario is invoked to recompute a prioritized list of Caregivers and subsequently re-invoke this Call for Help scenario with the updated list. |
| **Alternate / Exception flows** | A-1. (step 2): The selected Caregiver decides to decline the call:<br>a. The Edge System will select the next Caregiver from the prioritized list and send an emergency signal to him/her.<br>b. The flow continues at step 2 for the new Caregiver.<br>A-2. (step 2): The selected Caregiver accepts the call, but a voice connection with the Resident is not needed before heading over there:<br>a. The flow continues at sub flow S-1.<br>E-1. (step 3): The Caregiver and the Resident agree this is a false alert and no further action follows. |

| | |
|---|---|
| **Input data** | List of credentials for Smart Lock.<br>Prioritized list of Caregivers based on actual Resident and potential Caregivers' contexts. |
| **Output data** | Updated list of credentials for the SmartLock system.<br>Potentially additional context information about the Resident. |
| **Infrastructure** | Smart Lock connected to Edge System, Edge System with Internet access, Caregiver's Wearable with Internet access. |
| **Technical Building Blocks** | BB24.G_VEMCO: "Mobile Edge Computing"<br>BB24.I_UiO: "S-ABAC" |
| **Related SCOTT requirements** | 460 Data_processing_mode; 59 Standard-Based; 563 Catter for Contextual Auth.; 565 Rule-based; |

**Table 2 Description of Scenario 1**

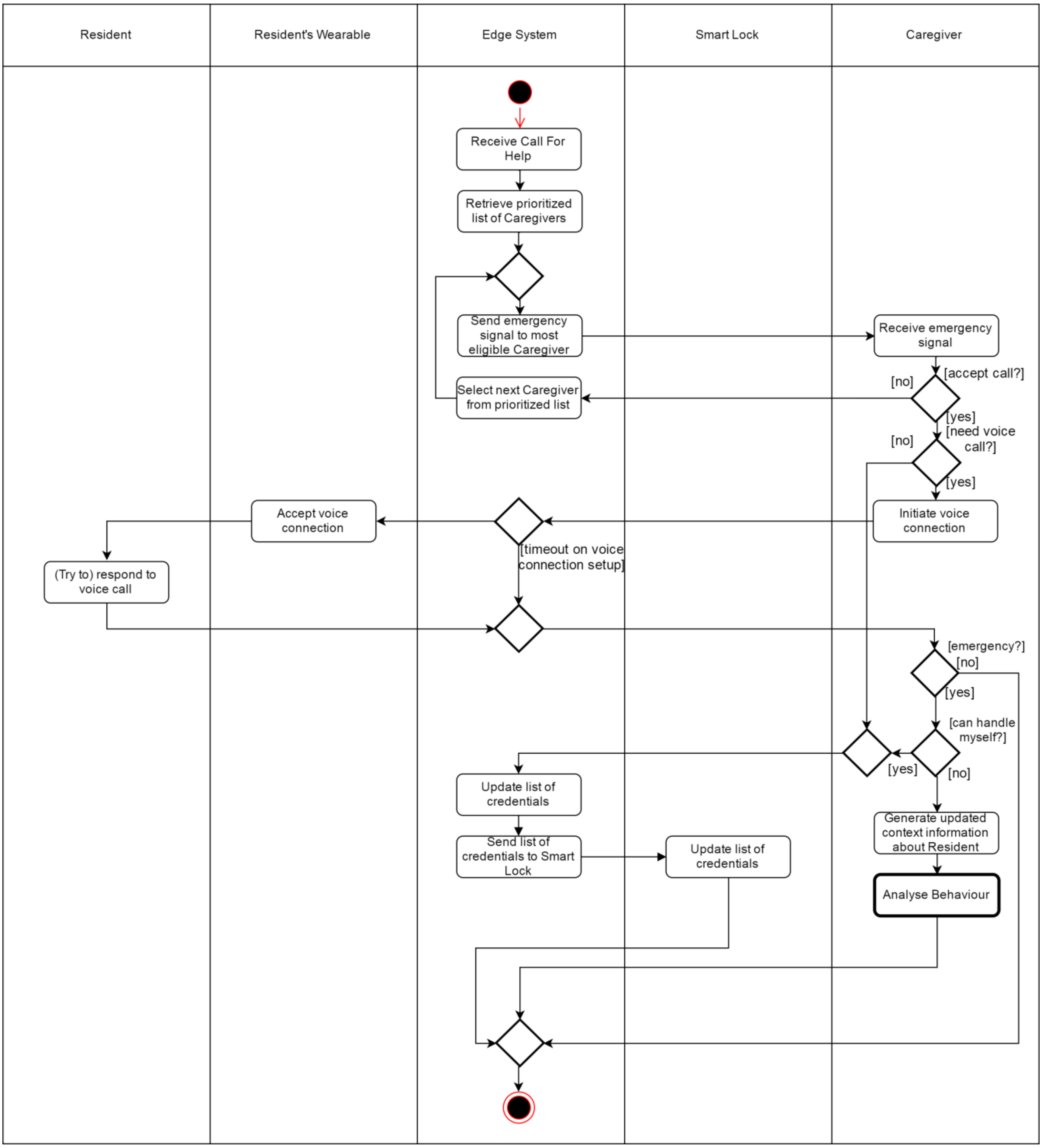

Resident
Resident's Wearable
Edge System
Smart Lock
Caregiver
Receive Call For Help
Retrieve prioritized list of Caregivers
Send emergency signal to most eligible Caregiver
Select next Caregiver from prioritized list
Receive emergency signal
[accept call?]
[no]
[yes]
[need voice call?]
[no]
[yes]
Initiate voice connection
Accept voice connection
(Try to) respond to voice call
[timeout on voice connection setup]
[emergency?]
[no]
[yes]
[can handle myself?]
[yes]
[no]
Update list of credentials
Send list of credentials to Smart Lock
Update list of credentials
Generate updated context information about Resident
Analyse Behaviour

**Figure 10 Activity diagram of Scenario 1**

### 3.4.2 Scenario 2: Update Resident Location

| | |
|---|---|
| **Use case** | WP21 Assisted Living and Community Care |
| **Scenario** | Update Resident Location |
| **Actors** | Multimodal Positioning System (MPS) – wants to keep information about the location of the Resident updated. |
| **Description** | This scenario describes how the Multimodal Positioning System updates a location of the Resident within the Edge System. |
| **Trigger** | Updating location of the Resident will be performed with a frequency defined in the Edge System. |
| **Normal flow of events** | 1. The Multimodal Positioning System gathers information about the Residents from one or more sources.<br>2. The Multimodal Positioning System estimates the location of the Resident.<br>3. The Multimodal Positioning System updates the location of the Resident in the System. |
| **Sub flows** | --- |
| **Alternate / Exception flows** | --- |
| **Input data** | Various Resident information needed to locate him/her. |
| **Output data** | Updated Resident location. |
| **Infrastructure** | The Resident's tag, smartphone or smartwatch; Edge System, MPS; Xetal sensors. |
| **Technical Building Blocks** | BB23.P_GUT: "Spatial-based authorization and authentication"<br>BB24.G_VEMCO: "Mobile Edge Computing" |
| **Related SCOTT requirements** | 390 Object localization and position; 391 Localization_method; 460 Data_processing_mode; |

**Table 3 Description of Scenario 2**

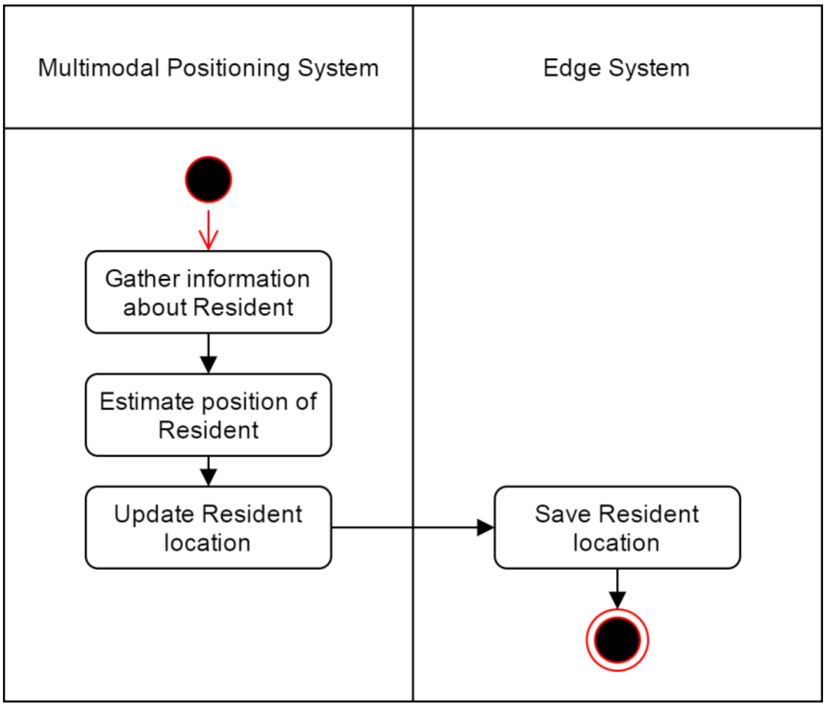

Multimodal Positioning System
Edge System
Gather information about Resident
Estimate position of Resident
Update Resident location
Save Resident location

**Figure 11 Activity diagram of Scenario 2**

### 3.4.3 Scenario 3: Analyse Resident Behaviour

| | |
|---|---|
| **Use case** | WP21 Assisted Living and Community Care |
| **Scenario** | Analyse Resident Behaviour |
| **Actors** | Context Reasoning System – wants to detect whether the Resident exhibits behaviour or is in a state that demands emergency intervention and infers from Resident and potential Caregivers‘ contexts who can most appropriately attend to the emergency. |
| **Description** | This scenario describes how the Context Reasoning System analyses behaviour of the Resident to determine whether there is an emergency and if so to derive a prioritized list of Caregivers. This list may include: informal Caregivers (e.g. next-of-kin, neighbours), formal Caregivers (e.g. visiting nurse, doctor, but also emergency call centers such as 112). |
| **Trigger** | Analysing behaviour of the Resident will be triggered by specific events (e.g. panic button push, fall detection, biometrics exceeding a threshold, geofences being crossed, staying for too long in a particular place) and/or performed periodically with a frequency defined in the Edge System. |
| **Normal flow of events** | 1. The Context Reasoning System gathers information about the Resident from the different sources e.g. panic button, location, fall detector and Smart Watch with vital-sign sensors.<br>2. The Context Reasoning System analyses the Resident’s behaviour on the basis of defined risks/dangers and determines whether there is an emergency or not:<br>a. If the system detects emergency: subscenario S-1 is performed.<br>b. Else: the scenario ends. |
| **Subflows** | S-1. The Context Reasoning System determined that there is an emergency situation:<br>a. Based on the context of Resident and potential Caregivers, the Context Reasoning System computes a prioritized list of Caregivers and sends an emergency warning to the Edge System.<br>b. The Edge System saves this prioritized list and invokes the Call for Help scenario. |
| **Alternate / Exeptional flows** | --- |
| **Input data** | Various sensor data relating to the Resident. Set of Caregivers associated to this Resident with their properties. |
| **Output data** | Prioritized list of Caregivers.<br>Trigger of the Call For Help scenario. |
| **Infrastructure** | Panic button, Vital-sign sensors, Fall detector, Multimodal Positioning System. |
| **Technical Building Blocks** | BB24.G_VEMCO: “Mobile Edge Computing” |
| **Related SCOTT requirements** | 460 Data_processing_mode; |

**Table 4 Description of Scenario 3**

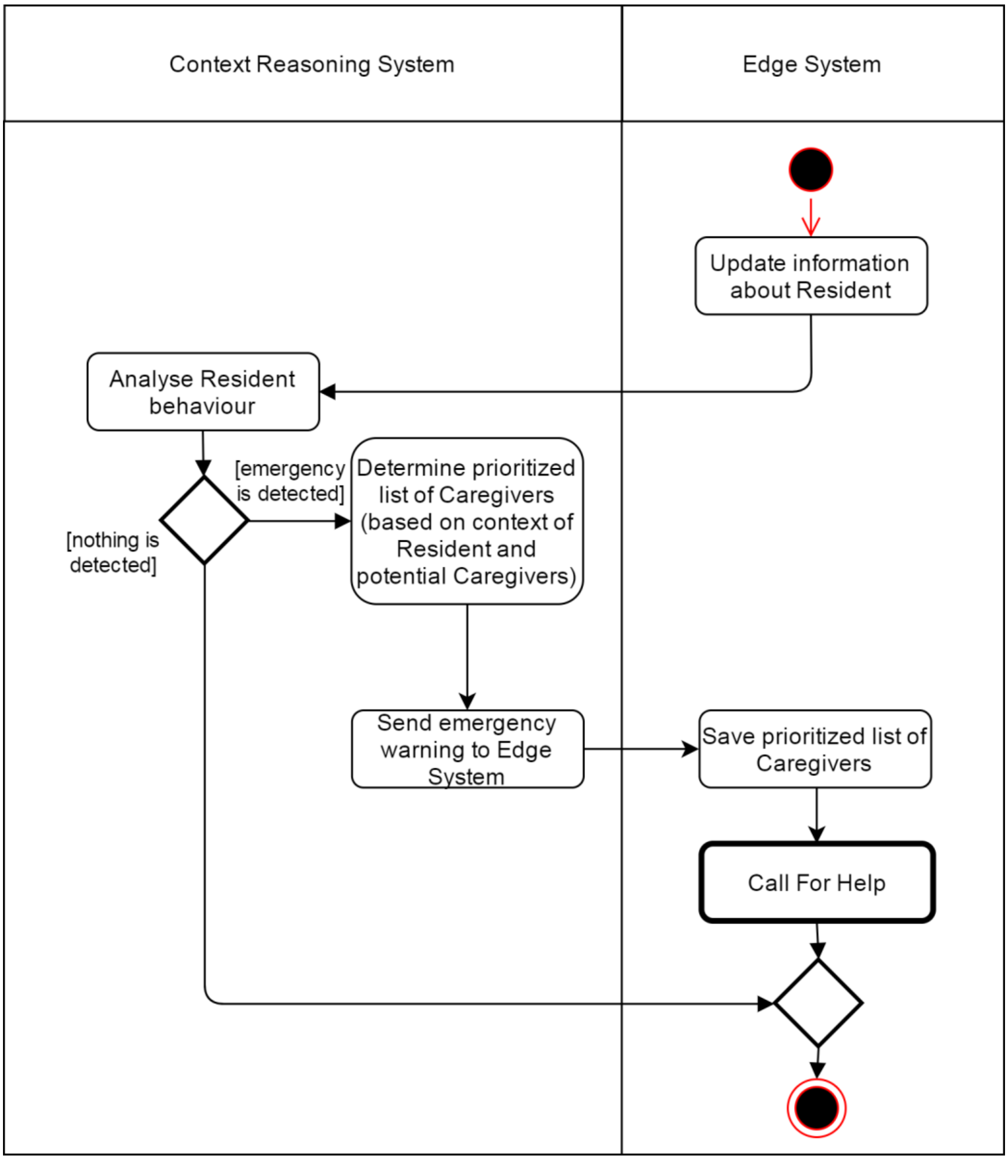

Context Reasoning System
Edge System
Update information about Resident
Analyse Resident behaviour
[emergency is detected]
Determine prioritized list of Caregivers (based on context of Resident and potential Caregivers)
[nothing is detected]
Send emergency warning to Edge System
Save prioritized list of Caregivers
Call For Help

**Figure 12 Activity diagram of Scenario 3**

### 3.4.4 Scenario 4: Enter Area

| | |
|---|---|
| **Use case** | WP21 Assisted Living and Community Care |
| **Scenario** | Enter Area |
| **Actors** | Caregiver– wants to enter the Resident’s area. |
| **Description** | This scenario describes a procedure of authorization and authentication at the entrance to the Resident’s area. |
| **Trigger** | The Caregiver approaches the entrance. |
| **Normal flow of events** | 1. The Caregiver uses his/her device to authorize.<br>2. The Smart Lock reads the authorization data and validates it. The Smart Lock accepts access and unlocks entry. |
| **Subflows** | --- |
| **Alternate / Exeptional flows** | E-1. (3) The ‘Caregiver’ hasn’t got the access rights:<br>a. Access is denied (i.e. the door remains locked). |
| **Input data** | List of credentials. |
| **Output data** | |
| **Infrastructure** | The Caregiver’s device with Bluetooth, Smart Lock. |
| **Technical Building Blocks** | BB23.P_GUT: “Spatial-based authorization and authentication”<br>BB24.I_UiO: “S-ABAC” |
| **Related SCOTT requirements** | 392 BYOD_concept; 399 Secure_resources_access; 59 Standard-Based; 563 Catter for Contextual Auth.; 565 Rule-based; |

**Table 5 Description of Scenario 4**

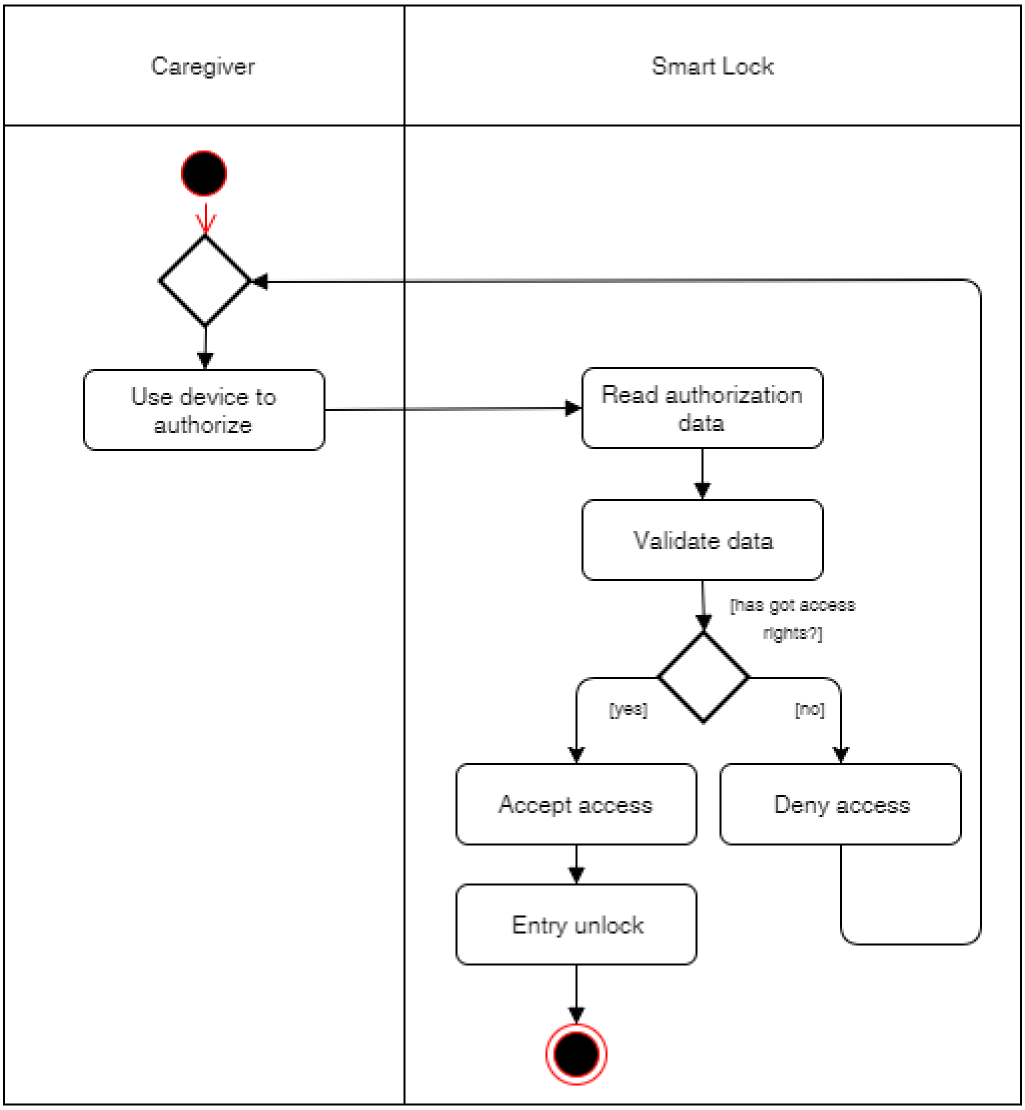


**Figure 13 Activity diagram of Scenario 4**

# 4 EXPLOITATION, DISSEMINATION AND STANDARDISATION

## 4.1 Exploitation

The topic of improving the trustworthiness of connected healthcare propositions and the promise of automated trust delegation in that respect has interest throughout Philips (**PRE**). PRE intends the use case on assisted living and community care, described in the current deliverable and targeted for the first iteration, which is to complete by M14, mainly as a carrier to explore the underlying technologies of automated trust delegation and context derivation. Based on the outcomes of those activities, specific business areas will get identified where those technologies could be exploited.

With regards to novel cellular connectivity (4.5G / 5G), PRE has identified some concrete use cases that stand to benefit significantly from these technologies. Specifically, 4.5G LPWAN technologies such as NB-IoT and Cat-M1 – as well as their 5G successor 5G-IoT – will enable the proliferation of cost effective devices for continuous patient monitoring that are comfortable to wear and last weeks, months or even years on a tiny battery. Furthermore, 5G is expected to bring ubiquitous localization, both indoors and outdoors, enabling breakthroughs in emergency care by localizing patients, elderly, caregivers and critical equipment alike. Both innovations will also radically improve asset management within and beyond care facilities.

Good examples of emergency care use cases that require ubiquitous, reliable and accurate localization, both indoors and outdoors, are the elderly care use case described in detail in Sections 3.2 – 3.4 (locate an elderly person wandering), the Sudden Cardiac Arrest use case sketched in Section 3.1 (locate bystanders, nearby layman responders and AED‘s) and the diabetes use case sketched by TellU in Appendix B (locate child with diabetes).

For any of these use cases, devices (i.e. 5G phones, AED, wearables) should be localized within a few meters, including height (necessary to determine the right floor). GPS is known to be insufficient indoors, but could be complemented by base station triangulation (3GPP Rel 14), provided that the base station density indoors is quite high (picocells). Alternatively, or additionally, the Wi-Fi Certified Location$^{TM}$ (possibly with IEEE 802.11az enhancements) of the building‘s Wi-Fi network could be seamlessly integrated with the 5G network through Wi-Fi cellular convergence.

No matter how location is estimated, privacy is a key concern that should be addressed through SCOTT innovations. The location of a particular individual should only be exposed to clearly identified individuals (i.e. Caregivers) for clearly identified  purposes (e.g. only in case of a suspected case of SCA, the 112 call center will be enabled to contact nearby layman responders).

The initial exploitation strategy assumes that most of the future exploitation-related actions will be initiated by Philips (PRE), which has the necessary organizational and economical potential and is one of the leading companies delivering high quality healthcare products globally. By merging ubiquitous localization technologies, 5G connectivity and access control paradigms together with SCOTT solutions that provide sufficient privacy and trustability to the end user, Philips will make an attempt to lead the development of innovative products that can be implemented on global scale. Within the domain, synergies will be determined between the following groups of partners:

- Large enterprises able to sell the final solutions (products, systems or services):
  - Philips
- Companies providing communication or cloud services:
  - TellU, Telenor
- SMEs providing innovative solutions:
  - Vemco, Xetal
- Research entities providing innovative technologies:
  - GUT, TU/e, UiO

The development of innovative products will be organized within WP21 use cases, in which technologies and products provided by different partners will be merged together to solve certain problems present in the healthcare domain. Once the next iteration of a use case is ready, it will be assessed by Philips and also relevant stakeholders (e.g. hospitals and representatives of clusters operating in the health domain) in order to properly address not only required functionality, but also privacy and trust concerns. It is envisioned, that after the project Philips will gather the most promising systems/products and assess possible ways to commercialize them.

**TellU** has the ambition to integrate project outcomes in its commercial services. TellU has selected diabetes as a focus area, as this is a domain where it is active already and will be working closely with several partners to deliver services that need trust delegation. In particular, TellU working with a Danish company, OpenTeleHealth, on developing device integration and patient app components for a system supporting patients with diabetes and their clinicians. The system is targeted at both Danish, European and international markets. TellU will also be working with a Norwegian company, Prediktor Medical, which has developed the BioMKR sensor for non-invasive continuous blood glucose measurement. Prediktor Medical has selected TellU to develop a data collection and processing service for this device.

## 4.2 Dissemination

Dissemination of the healthcare domain results is tightly connected to the initial exploitation strategy. First, use cases together with underlying technologies will be presented to appropriate stakeholders that will be connected to the SCOTT ecosystem to receive early feedback. To this end, two groups of stakeholders will be determined:

- Healthcare-oriented organizations/clusters, to properly address/verify required functionalities of the final solutions/products, as well as possible privacy and trust concerns.
- Clusters of ICT companies, to involve SME companies that may provide complementary technologies to enrich the final solutions/products.

Specifically, GUT is exploring opportunities within Poland to secure a location, which will be open to all WP21 partners and where the WP21 demonstrator(s) can be hosted in a natural environment. This location will benefit dissemination, as well as exploitation (e.g. by organizing demonstrations for potential customers).

Additionally, research partners will publish the most valuable scientific results in journals and conferences to gather attention from other researchers and stimulate further development of the underlying technologies. To achieve the highest impact, scientific partners plan to publish their results in IEEE Access (new multidisciplinary Open Access journal with IF=3.244), SENSORS, Journal of Medical Internet Research – Mobile Health and Ubiquitous Health, Personal and Ubiquitous Computing (Springer), Smart Health (Elsevier), IEEE Internet of Things Journal, Antenna and Wireless Propagation Letters.

The initial dissemination plans of the healthcare domain partners include:

- **PRE** has initiated contacts with the Dutch Ministry of Economic Affairs and related initiatives such as “Partnering for Trust” and “Zeker-Online” to discuss privacy labelling, as those bodies have worked on privacy labelling before in cooperation with German and French authorities. Through those contacts SCOTT could set a baseline and learn from prior work in the area, while at the same time gaining wider exposure for some of its main ambitions. Note that those contacts have a wider scope than just the health domain (i.e. just WP21).
- **GUT** will publish the major results in journals (mainly open access) and international conferences and will also present project achievements at workshops/meetings (e.g. during conferences,

symposia, etc) and fairs. Additionally, GUT will disseminate project outcomes among relevant bodies (i.e. stakeholders) and coordinate stakeholders engagement actions in Poland.

- **TU/e** will regularly publish SCOTT results in open access journals as well as in prestigious conference and workshop proceedings. TU/e researchers will attend international conferences where these papers are published to present the results to an audience (typically from academy and industry). TU/e will produce PhD and master theses based on SCOTT results. TU/e will present a SCOTT poster at the Data Science Center Eindhoven (DSC/e) yearly summit (December 4, 2017), summarizing SCOTT WP21 ambitions, progress and goals.
- **VEMCO** will hold a series of meetings with their business partners from different domains in order to discuss healthcare issues. That will allow finding potential threats in other domains and make the developed solution reusable.
- **TellU** disseminates WP21 prototypes and results in e-health conferences and other relevant events. For example, events organised by Norway Health Tech. TellU is member of Norway Health tech and they are regularly organising eHealth events. While TellU does not plan for own papers, it will contribute to research papers, in particular for the validation part based on use case and findings.
- **UiO**'s dissemination activities include publication of international conference and journal papers which, in addition to solving the open challenges and problems, give a roadmap and framework for further research. Other activities include organizing related conferences and workshops, as well as presenting talks and courses on SCOTT topics. As part of transferring the theoretical research into innovation and commercialization, UiO aims to provide software and applications to be applicable within the SCOTT domains and facilitates interoperability between existing and new technologies. In order to make the project and its activities widely disseminated, and to raise awareness and inform society about the challenges and opportunities related to the SCOTT project, all activities, such as organized meetings including industrial and technical meetings, publications and presentations, student supervisions, and other ongoing events and contributions are accessible on a website [3]. Useful links to other projects related to SCOTT, such as the IoTSec project, are also made available and connected through this website. Every related UiO staff member attending the projects and academic groups is also linked to the projects and reflected in the dissemination activities. Specifically:
    1. UiO plans to publish in journals related to IoT and health, e.g., Journal of Medical Internet Research – Mobile Health and Ubiquitous Health; Personal and Ubiquitous Computing (Springer); Smart Health (Elsevier); IEEE Access; IEEE Internet of Things Journal.
    2. Conferences that UiO usually plans to attend in IoT and health are: ACM Conference on Pervasive and Ubiquitous Computing (UbiComp); IEEE International Conference on Pervasive Computing and Communications (PerCom); International Conference on Pervasive Computing Technologies for Healthcare. Two contributions to conferences and workshops are (about to be) published [4][5].
    3. UiO is actively promoting SCOTT in various adjacent activities that we are involved in. In particular, UiO is disseminating SCOTT in other relevant projects it is engaged in, including IoTSec, DiversIoT, and RailCons. UiO is also promoting SCOTT when meeting authorities, like the Data protection authorities, Consumer protection authorities, and the NVE Directorate for Energy. UiO is creating relevant MSc topics, and has also attracted one PhD student from the department to work on SCOTT related topics. UiO is trying to attract external international collaborators on SCOTT related topics; e.g., Chalmers University Sweden.

- **Xetal** is planning to disseminate results by means of newsletters and social media articles. Depending on the results Xetal will consider publications in journals and/or conferences related to lifestyle monitoring or sensors at large.

## 4.3 Standardization

The standardization approach for the health domain is already clearly outlined in SCOTT deliverable D31.1 concerning the standardization approach [6]:

> *Within the Health Domain (WP21) a variety of connected vital-sign sensors will be explored. Specifically, so-called Direct-to-Cloud connectivity through cellular networks will enable hassle-free (no gateway!), reliable connectivity, anytime and anywhere, even for devices running from a coin cell battery. This can optionally be complemented by accurate indoor and outdoor localization. Although some of these features can already be realized with recent 4G (also coined as 4.5G) technology (e.g. NB-IoT and Cat-M1), much is expected from the upcoming generation of cellular networks, 5G. The EU is currently looking towards vertical industries, including healthcare, to influence 5G standardization by generating requirements for future cellular networks that best support those industries. In this perspective, it should be noted that 5G – much more than any of its predecessors – will be a palette of technology options enabling a wide range of trade-offs between key performance indicators such as throughput, latency and power consumption. Making sure the right trade-offs are available for IoMT (Internet of Medical Things) devices including, but not limited, to vital-sign sensors is pivotal to the take-up of 5G for future healthcare. Specifically, SCOTT members should participate in 5G PPP activities to keep a close link to the 5G ecosystem in Europe. In this perspective, BB24.L regarding Adaptive Network Slicing – a key topic in 5G to better manage security and QoS – and BB24.G regarding Mobile Edge Computing are also important to mention.*
>
> *Trust Delegation will be one of the key innovations from WP21. Amongst others, it will put the patient (or user) in control of his personal health record, a very important aspect to instil trust in highly connected healthcare propositions. SCOTT members should maintain close ties to organizations such as the Personal Connected Health Alliance, HL7/FHIR and AIOTI (WG5 and WG7, in particular) to monitor developments and spot opportunities to influence future standardization based on SCOTT results. In this perspective, BB23.P regarding Spatial Based Authorization and Authentication and BB24.I regarding Semantic Attribute Based Access Control are also important to mention.*

# 5 INTEROPERABILITY

Interoperability in WP21 may be considered from different perspectives. The first perspective is the architecture pattern presented in Section 3.2. The presented initial version of the architecture allows for fast and efficient integration with third party components. This allows for fast and efficient integration with any Building Block which is considered valuable and relevant for WP21.

On the other hand, interoperability is addressed directly in SCOTT through the Building Block approach. Such a concept is designed for raising the interoperability level through utilization in various domains and work packages. WP21 Building Blocks follow this approach, examples are given below:

- BB23.P Component – Multimodal Positioning System – is utilized in different Work Packages from different domains (WP9, WP12, WP15, WP21). In each of these WP’s, the component is responsible for delivering accurate information about an object’s current position. Another BB23.P component, Access Control System, is to be implemented in WP9, WP15 and WP21.
- BB24.I – Semantic attribute-based access control – is applied in different Use Cases from different domains such as WP8, WP11, WP15 and WP21. In each of these Use Cases, the related application is responsible for authorization and access control in a different context, which is determined based on different attributes and the semantic rules specifying the context.

Finally, regarding the health domain, interoperability plays a role at various interfaces. Standardization should help provide interoperability, as outlined in Section 4.3.

# 6 LINK TO TECHNOLOGY LINES

The use case work described in the current deliverable is linked to theTechnology Lines TL1 “Security and Safety” and TL2 “Distributed Cloud Integration” through their respective Technical Building Blocks BB23.O, BB23.P, BB24.G, BB24.I and BB24.L.

For more details please refer to the overview in Table 1 and the specific TBB links mentioned in each of the scenarios described in Table 2, Table 3, Table 4 and Table 5. See furthermore Sections 2.3.6 and 2.3.7.

# 7 CONCLUSIONS

An iterative approach towards exploring trust delegation in the healthcare domain is proposed addressing the two ‘template’ use cases ‘patient trend monitoring’ and ‘emergency handling’. Trust delegation enables a patient or individual at risk to determine who can access what (medical data, access to home, etc) under which circumstances, all in a very trustful, transparent and intuitive manner.

For the first iteration – aiming at a first demonstrator in M14 – a specific use case in assisted living and community care is worked out in more detail. It enables frail elderly people – who are e.g. prone to falling – to remain living in the comfort of their own home longer, in an attempt to curb the ever soaring costs of healthcare and an aging population. The solution involves a personal emergency response system using multi-modal sensoric information to infer the context of the elderly resident, as well as that of potential caregivers, to determine the most appropriate caregiver to help. In many cases, this could be an informal caregiver enabling less costly – and more trustful – exploitation of the personal emergency response system. The most critical scenarios are worked out in detail with activity diagrams and a first multi-view architecture is sketched.

Avoiding costly intervention of a centralized call center, unless absolutely necessary, and processing all privacy sensitive data through on-premise edge computing constitute the major progress beyond the state-of-the-art.

# 8 REFERENCES

[1] SCOTT Description of Work, Grant Agreement Number 737422, 2017-05-12.

[2] Elderly pays fine for falling (in Dutch), Eindhovens Dagblad, https://www.ed.nl/binnenland/oudere-betaalt-boete-voor-valpartij~a0523fd0/, [2017-11-04].

[3] Secure Connected Trustable Things – SCOTT JU ECSEL project – Norwegian contribution, http://its-wiki.no/wiki/SCOTT:Home, [2017-11-04].

[4] Toktam Ramezanifarkhani, Peyman Teymoori, “Securing the Internet of Things with Recursive InterNetwork Architecture (RINA)”, to be published in the proceedings of International Conference on Computing, Networking and Communications, (ICNC 2018), Maui, Hawaii, USA, March 5-8, 2018.

[5] Toktam Ramezanifarkhani, Elahe Fazeldelkordi, Olaf Owe, “A Language-Based Approach to Prevent DdoS Attacks in Distributed Object Systems”, in 29th Nordic Workshop on Programming Theory (NWPT ‘17), 01-03 November 2017, Åbo Akademi Univesrsity, Turku.

[6] SCOTT Deliverable D31.1 “Standardization/Regulation/Certification Approach of SCOTT”, v1.0. 2017-09-25.

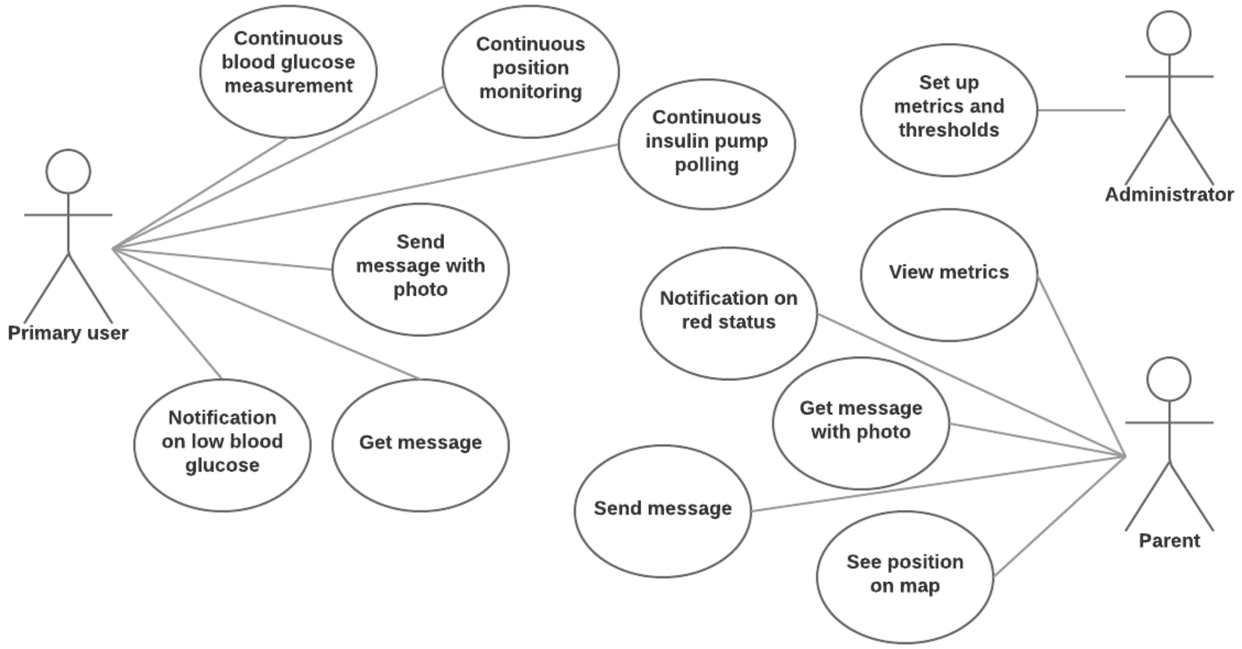
# A. ABBREVIATIONS AND DEFINITIONS

| Term | Definition |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 4G | Fourth generation of cellular networks, also known as LTE (current generation of 3GPP standards) |
| 4.5G | Recent 3GPP technologies such as NB-IoT and Cat-M1 that still fall under 4G/LTE |
| 5G | Fifth generation of cellular networks (upcoming generation of standards by 3GPP) |
| 5G-IoT | 5G successors of narrowband / massive IoT standards like NB-IoT and Cat-M1 |
| AED | Automatic External Defibrillator |
| AIOTI | Alliance for Internet of Things Innovation |
| ALCSS | Assisted Living and Community Care System |
| BioMKR | Smart watch product under development by Prediktor Medical, capable of CGM |
| BLE | Bluetooth Low Energy |
| Cat-M1 | 3GPP standard for low-bandwidth communications (4.5G); higher bandwidth than NB-IoT |
| CGM | Continuous Glucose Monitoring |
| CPR | CardioPulmonary Resuscitation |
| FHIR | Fast Healthcare Interoperability Resources |
| GDP | Gross Domestic Product |
| GPS | Global Positioning System |
| HL7 | Health Level Seven International; the world-wide standard for secure electronic information exchange in healthcare |
| IoMT | Internet of Medical Things |
| IoT | Internet of Things |
| IR | InfraRed |
| LTE | Long Term Evolution (synonymous to 4G) |
| MPS | Multimodal Positioning System |
| NB-IoT | Narrow Band IoT; 3GPP standard for low-bandwidth communications (4.5G) |
| SCA | Sudden Cardiac Arrest |
| TBB | Technical Building Block |
| TelluCloud | Cloud platform for creating products and services marketed by TellU |
| UML | Universal Modelling Language |
| WDA | Wireless Data Aggregator |

# B. USE-CASE: CHILD WITH TYPE 1 DIABETES (TELLU)

Charlotte is 10 years old and has diabetes type 1. Her mother and father have received guidance to manage a child with diabetes. Charlotte has an insulin pump injecting her insulin. She needs to enter occasional blood glucose measurements, as well as the calorie count for all the food she will eat, into the pump, and it adjusts insulin dosage based on this information and the settings made by her doctor. She wears the BioMKR wrist sensor for continuous measurement of blood glucose, but also pricks her finger two times a day to get an accurate measurement and calibrate the BioMKR. She often needs to call her parents when she is out on her own, to ask for help calculating calories for what she will eat. Charlotte's parents worry about her glucose level going too low at night or when she is playing away from the house. Connecting the BioMKR and GPS position of her phone to the TelluCloud system gives them a possibility to monitor her. However, for privacy reasons they should not monitor her more than strictly necessary, and so her position is only shared if there is an emergency (low blood sugar).

**Infrastructure/equipment for primary user:** Smartphone with app, insulin pump, blood glucose meter, BioMKR sensor.


Continuous blood glucose measurement
Continuous position monitoring
Continuous insulin pump polling
Set up metrics and thresholds
Administrator
Primary user
Send message with photo
View metrics
Notification on red status
Get message with photo
Parent
Notification on low blood glucose
Get message
Send message
See position on map

## Scenario 1: Continuous monitoring

**Trigger:** This scenario is running continuously. Charlotte can open the app to access the status and data.

**Normal flow:**

1. The smartphone has a BLE connection to the BioMKR sensor, and the app gets regular blood glucose numbers all day and night, except when it is charging. The data is sent to the cloud.
2. The app uses the GPS positioning of the phone (with network position as back-up) to get regular position fixes. The data is also sent to the cloud, but not made available to human users unless there is an emergency.
3. The app also regularly polls the insulin pump for data, getting the calories Charlotte has entered and the insulin injected. This is also sent to the cloud. Note that this is only to make it more readily available to parents and health professionals – the system does not do reasoning or alerts based on this data, and there is no feedback from our system to the pump.

4. When Charlotte opens the app, she can check that all is well. It shows a green/yellow/red status for her blood glucose as well as for connected devices. However, she does not need to check this herself, as this information is also made available to her parents, and they are notified if not all is well.

**Alternate/Exception flows:**

There are a number of things which could be in a non-optimal state (yellow or red). Charlotte's parents are notified of a red state, and will need to contact her to help resolve the situation.

- Blood glucose low: See scenario 3.
- BioMKR unavailable: This could be a BLE connectivity issue, or the sensor's battery could be empty. Battery status is monitored, so the system will know if it's the battery. Charlotte's parents will need to help resolve connectivity issues.
- BioMKR faulty readings: The system will check if values are reasonable, to filter out any obviously wrong values and mark the device as having a yellow or red status.
- Position unavailable: The app may only get a (less accurate) network position when Charlotte is indoors, which is fine. There is only an alarm if the app is unable to get any position data for a prolonged period of time, which is highly unlikely and should only happen if the app is denied position information in the phone settings.
- Insulin pump unavailable: This is similar to the BioMKR problem, and handled in a similar way, although it is less critical.
- No server connection: If the app is unable to post data to the cloud, this will be detected on the server side once a time limit is reached without any data from the app, so that the parents can also be notified of this. If this condition persists, Charlotte's last known position will be made available to her parents.

**Postconditions:** Measurements of blood glucose, as well as calories, insulin and position are transmitted to the cloud and stored there, available to Charlotte's parents when needed.

## Scenario 2: Help with food

**Trigger:** Charlotte is at the birthday of a friend, where she is given pizza and cake. She needs help calculating calories to enter in the insulin pump.

### Normal flow

1. Charlotte opens the app, and selects to "Send photo".
2. The camera screen of the phone is activated, and Charlotte takes a picture of a pizza slice. She acknowledges sending of the photo, which means her parents will get it in their apps.
3. She repeats the process for a piece of cake.
4. She gets a message from her father in the messaging section of the app, saying how many calories he thinks the pizza slice and piece of cake represents.
5. Charlotte enters the combined calories of what she intends to eat into the insulin pump.
6. As usual, the calories and insulin will later be picked up by the app from the pump.

### Alternate/Exception flows

The parents can see each other's messages, if they need to coordinate their answers. If no one answers, there may be additional contacts in the system, such as a grand-parent, although Charlotte will probably try calling her parents.

**Postconditions:** Charlotte gets the correct amount of insulin and eats the pizza and cake. Calories and insulin are transmitted to the cloud and stored there.

## Scenario 3: Alarm on low blood glucose

**Trigger:** The BioMKR sends a blood glucose update to the app once a minute and this is passed on to the server side. Now the value is dangerously low while Charlotte is outside playing.

### Normal flow

1. The app gets the blood glucose reading from the BioMKR sensor, and passes it on to the cloud. The latest GPS position is included in the message.
2. With the value being dangerously low, it is marked as red in the app. The phone gives off a notification, but Charlotte is already very weak.
3. Charlotte's mother is at home and gets a notification in her app. Since this is a red alert, Charlotte's position is made available to her, so she can see where she is in a map.

**Alternate/Exception flows**

The phone may be unable to get a GPS fix around the time of the low blood glucose reading. It will then use a low-accuracy network position, which may not be of much help to find Charlotte. But the system has the history of previous GPS positions, which can then be made available to Charlotte's mother in the emergency.

**Postconditions:** Charlotte's mother is alerted of the low blood sugar and position, and goes out to get her daughter and give her sugar.