



Horizon 2020
Programme

H2020-SU-TDS-02-2018

Trusted digital solutions and Cybersecurity in Health and Care



ProTego

DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND
CARE CENTERS

Project N° 826284

ProTego

***D2.3 - Final description of business requirements,
scenarios, use cases, metrics, and processes***

Responsible: OSR

Contributors: Pietro Vismara, Michele Cantarutti,
Diana Trojaniello, Salvador Garcia Torrens,
Dave Singelee, Eliot Salant, Carlos Cilleruelo Rodríguez,
Luis Carrascal Crespo, Steve Taylor, Esteban Municio,
Noel Tomas

Document Reference: D.2.3

Dissemination Level: Confidential

Version: 1.0

Date: 30/04/2021

Executive summary

This document serves as the final specification of the business requirements, scenarios and use cases of the ProTego toolkit, in addition to finalizing the description of the metrics adopted to assess the appropriateness of the achieved solution. In continuity with the Description of the Action, we comment on the business requirements of the ProTego project and contrast them against their anticipated impact on healthcare organizations. Moreover, we discuss potential stakeholders of the project and reiterate on possible risks to the second part of the project. After that, we characterize the ProTego solution in terms of its functionalities, and consequently delimit the scope of its final release. Next, we detail the user requirements for the project. More precisely, we identify user classes of interest, and then distil their characteristics in order to construct user personas, which are fictitious, yet representative users for whom the solution is built. After listing relevant user roles, we proceed by illustrating the main scenarios of interactions with the ProTego toolkit, which are consequently generalized as a set of use cases. We conclude the requirements part by identifying the quality attributes of interest for the ProTego toolkit. The second part of this document is instead devoted to the presentation of the demonstration platform for the project. We first introduce FoodCoach, a food recommendation system that suggests *personalized nutrition plans* to end-users. In this respect, we report a similar analysis to that conducted for ProTego itself. More specifically, after presenting FoodCoach's stakeholders, we detail its user personas, roles and use cases. We then present Pocket EHR, a platform that allows both patients and physicians to access relevant data stored as part of the hospital electronic health records. Again, we analyze such a case study in terms of its stakeholders, user personas, roles and use cases. Both FoodCoach and Pocket EHR will interact with the hospital infrastructure by means of ProTego, to which they will defer crucial application concerns, such as storage of medical data. In this respect, we present a number of real-life situations in which patients' safety, data privacy and infrastructures may be put at risk and how ProTego can assist in reducing such a risk. The last part of the document is dedicated to the final description of the metrics that have been specified in order to evaluate the achievement of the project's objectives and to provide a valuable indication of the project success.

Differences from Version 2 of D2.2

Deliverable 2.3 extends and revises Deliverable 2.2 V2 in several aspects:

- **Section III** has been extended with a comprehensive storyboard and its related use cases that encompass the different steps of the deployment and installation process of the ProTego toolkit. Moreover, we included a step related to the configuration of the mobile device, in order to set up the continuous authentication agent. The configuration of the toolkit has also been reviewed taking into account the outcome of D7.3. In light of this consideration, the possibility to specify the query templates has been removed in favor of a user-centric access control. Additionally, we described new interactions with the IoT device, which in turn stem from new technological choices. Lastly, we improved the description of the overall process, to reflect the fact that some responsibilities that were originally meant to be handled by a centralized system have been subsequently offloaded to the single components of the ProTego toolkit.
- **Section IV** has been modified in accordance with the results of D7.3. In this fashion, we updated the list of quality attributes by removing those related to the configuration of the query templates. Additionally, we reviewed the qualities associated with the updated description of the IoT device.
- **Section VII** has seen some changes to illustrate the introduction of the updated security mechanism adopted for the IoT device. These changes affected the description of the following real-life situations: “Sniffing traffic from IoT device” and “Spoofing IoT device”.
- **Section VIII** now includes a paragraph dedicated to the specification of the non-functional success rate. This part finalizes the description of the metrics adopted to evaluate the achievement of the project’s objectives.

Contributors Table

| DOCUMENT SECTION | AUTHOR(S) | REVIEWER(S) |
|---------------------|--|---|
| I-V, VIII-IX | Pietro Vismara, Michele Cantarutti, Diana Trojaniello (OSR) | Antonio Jesús Gamito González (Inetum), Luis Carrascal (Inetum), Salvador García (MS) |
| VI | Salvador Garcia Torrens (MS), Pietro Vismara, Michele Cantarutti (OSR) | Antonio Jesús Gamito González (Inetum), Luis Carrascal (Inetum), Salvador García (MS) |
| VII | Dave Singelee (KUL), Carlos Cilleruelo Rodríguez (UAH), Eliot Salant (IBM), Pietro Vismara, Michele Cantarutti (OSR), Luis Carrascal (Inetum), Esteban Municio, Noel Tomas | Antonio Jesús Gamito González (Inetum), Luis Carrascal (Inetum), Salvador García (MS) |

Table of Contents

| | |
|--|------------|
| I. BUSINESS REQUIREMENTS | 9 |
| I.1. BACKGROUND..... | 9 |
| I.2. OBJECTIVES | 10 |
| I.3. STAKEHOLDERS..... | 12 |
| I.4. RISKS..... | 13 |
| II. SCOPE | 14 |
| II.1. FEATURES | 14 |
| II.2. FINAL RELEASE | 14 |
| III. USER REQUIREMENTS | 16 |
| III.1. PERSONAS | 16 |
| III.2. STORYBOARD..... | 18 |
| III.3. ROLES | 32 |
| III.4. USE CASES..... | 33 |
| IV. QUALITY ATTRIBUTES | 53 |
| IV.1. AUTHENTICITY..... | 53 |
| IV.2. INTEGRITY | 54 |
| IV.3. NON-REPUDIATION | 56 |
| IV.4. CONFIDENTIALITY | 57 |
| IV.5. AVAILABILITY | 58 |
| IV.6. AUTHORIZATION..... | 58 |
| IV.7. DETECTABILITY | 59 |
| IV.8. DATA PROTECTION | 60 |
| V. NUTRITIONAL CASE STUDY | 61 |
| V.1. OVERVIEW..... | 61 |
| V.2. STAKEHOLDERS..... | 62 |
| V.3. PERSONAS | 63 |
| V.4. STORYBOARD..... | 66 |
| V.5. ROLES..... | 72 |
| V.6. USE CASES..... | 73 |
| VI. ELECTRONIC HEALTH RECORD CASE STUDY | 79 |
| VI.1. OVERVIEW | 79 |
| VI.2. STAKEHOLDERS..... | 80 |
| VI.3. PERSONAS | 81 |
| VI.4. STORYBOARD | 84 |
| VI.5. ROLES..... | 88 |
| VI.6. USE CASES..... | 89 |
| VII. REAL-LIFE SITUATIONS | 94 |
| VII.1. STEALING A DEVICE | 95 |
| VII.2. UNAUTHORIZED REQUEST | 97 |
| VII.3. TAMPERING WITH MEDICAL DATA | 99 |
| VII.4. SNIFFING TRAFFIC FROM IOT DEVICE | 103 |
| VII.5. SPOOFING IOT IDENTITY | 105 |
| VIII. METRICS | 107 |
| VIII.1. FUNCTIONAL SUCCESS RATE | 107 |
| VIII.2. NON-FUNCTIONAL SUCCESS RATE | 121 |
| VIII.3. USABILITY METRICS..... | 131 |
| IX. CONCLUSIONS | 134 |

X. REFERENCES AND INTERNET LINKS135

Table of Figures

Figure 1. The relationship between objectives, the features enabling them and their impact 11
 Figure 2. Stakeholder map of the ProTego toolkit..... 12
 Figure 3. Feature tree of the ProTego toolkit 15
 Figure 4. Use case diagram of the ProTego toolkit..... 33
 Figure 5. FoodCoach homepage 61
 Figure 6. Stakeholder map of the FoodCoach platform 62
 Figure 7. Use case diagram of the FoodCoach platform 73
 Figure 8. Stakeholder map of Pocket EHR 80
 Figure 9. Use case diagram of Pocket EHR..... 89
 Figure 10. ProTego, FoodCoach and Pocket EHR personas, including the attacker 107
 Figure 11. Goal-question-metric (GQM)..... 121
 Figure 12. After-Scenario Questionnaire (ASQ) administered via a Web interface 132
 Figure 13. System Usability Scale (SUS)..... 132

List of Tables

Table 1. Major features of the ProTego toolkit 14
 Table 2. Carlo, the “Network operator” persona 16
 Table 3. Andrew, the “IT infrastructure manager” persona 17
 Table 4. Storyboard between stakeholders, as mediated by ProTego 18
 Table 5. User roles of the ProTego toolkit..... 32
 Table 6. “Deploy cluster” use case 34
 Table 7. “Install Data Gateway” use case 34
 Table 8. “Install Network Slicing” use case 35
 Table 9. “Install SIEM” use case..... 35
 Table 10. “Install SSM” use case..... 36
 Table 11. “Install Continuous authentication” use case 36
 Table 12. “Register user in a component” use case 37
 Table 13. “Conduct first-time risk assessment” use case 37
 Table 14. “Assess prospective risks to the infrastructure” use case 38
 Table 15. “Install application” use case 39
 Table 16. “Configure application network slices” use case..... 40
 Table 17. “Configure application logging mechanism” use case 41
 Table 18. “Specify application access control” use case 42
 Table 19. “Configure mobile device” use case..... 42
 Table 20. “Store initial medical data” use case 43
 Table 21. “Register mobile device” use case 44
 Table 22. “Store medical data” use case..... 45
 Table 23. “Retrieve medical data” use case..... 46
 Table 24. “Assign IoT device to application user” use case 47
 Table 25. “Log custom application event” use case..... 48
 Table 26. “Send medical data securely” use case 49
 Table 27. “Report suspicious activity” use case..... 50
 Table 28. “Respond to alert” use case 50
 Table 29. “Review alerts” use case 51
 Table 30. “Review new risk evaluation” use case 51
 Table 31. “Reflect infrastructure changes” use case 52

| | |
|--|-----|
| Table 32. Authenticity requirements | 53 |
| Table 33. Integrity requirements | 54 |
| Table 34. Non-repudiation requirements | 56 |
| Table 35. Confidentiality requirements | 57 |
| Table 36. Availability requirements | 58 |
| Table 37. Authorization requirements | 58 |
| Table 38. Detectability requirements | 59 |
| Table 39. Data protection requirements | 60 |
| Table 40. Elisa, the “nutritionist” persona | 63 |
| Table 41. Antonella, the “patient” persona | 64 |
| Table 42. Manuel, the “admin” persona | 65 |
| Table 43. Storyboard between the patient and the nutritionist, as mediated by FoodCoach | 66 |
| Table 44. User roles of the FoodCoach platform | 72 |
| Table 45. “Register nutritionist” use case | 74 |
| Table 46. “Unregister nutritionist” use case | 74 |
| Table 47. “Register patient” use case | 74 |
| Table 48. “Register patient’s examination” use case | 75 |
| Table 49. “Prepare patient’s Personalized Nutrition Plan” use case | 75 |
| Table 50. “Publish new patient’s prescription” use case | 76 |
| Table 51. “Access statistics” use case | 76 |
| Table 52. “Obtain device data” use case | 76 |
| Table 53. “Get food suggestions” use case | 77 |
| Table 54. “Register food consumption” use case | 77 |
| Table 55. “Register weight measurement” use case | 77 |
| Table 56. “Access personal statistics” use case | 78 |
| Table 57. Julio, the “physician” persona | 81 |
| Table 58. Javier, the “patient” persona | 82 |
| Table 59. Iago, the “admin” persona | 83 |
| Table 60. Storyboard between the patient and the physician, as mediated by Pocket EHR | 84 |
| Table 61. User roles of the Pocket EHR platform | 88 |
| Table 62. “Register physician” use case | 90 |
| Table 63. “Unregister physician” use case | 90 |
| Table 64. “Register patient” use case | 91 |
| Table 65. “Unregister patient” use case | 91 |
| Table 66. “Read patient’s registered data” use case | 91 |
| Table 67. “Review alarms for assigned patients” use case | 92 |
| Table 68. “Check for future appointments” use case | 92 |
| Table 69. “Check the result of a test” use case | 92 |
| Table 70. “Report health status information” use case | 93 |
| Table 71. Real-life situations overview | 94 |
| Table 72. “Stealing a device” real-life situation | 95 |
| Table 73. “Unauthorized request” real-life situation | 97 |
| Table 74. “Tampering with medical data” real-life situation | 99 |
| Table 75. “Sniffing traffic from IoT device” real-life situation | 103 |
| Table 76. “Spoofing IoT device” real-life situation | 105 |
| Table 77. Acceptance tests of the “Deploy cluster” use case | 108 |
| Table 78. Acceptance tests of the “Install Data Gateway” use case | 108 |
| Table 79. Acceptance tests of the “Install Network Slicing” use case | 108 |
| Table 80. Acceptance tests of the “Install SIEM” use case | 109 |
| Table 81. Acceptance tests of the “Install Continuous Authentication” use case | 109 |
| Table 82. Acceptance tests of the “Install SSM” use case | 109 |
| Table 83. Acceptance tests of the “Register user” use case | 110 |
| Table 84. Acceptance tests of the “Conduct first-time risk assessment” use case | 110 |
| Table 85. Acceptance tests of the “Assess prospective risks to the infrastructure” use case .. | 110 |
| Table 86. Acceptance tests of the “Install application” use case | 111 |
| Table 87. Acceptance tests of the “Configure application network slices” use case | 111 |
| Table 88. Acceptance tests of the “Configure application logging mechanism” use case | 112 |

Table 89. Acceptance tests of the “Specify application access control” use case 112
 Table 90. Acceptance tests of the “Configure mobile device” use case..... 112
 Table 91. Acceptance tests of the “Store initial medical data” use case 113
 Table 92. Acceptance tests of the “Register mobile device” use case 114
 Table 93. Acceptance tests of the “Store medical data” use case..... 115
 Table 94. Acceptance tests of the “Retrieve medical data” use case..... 116
 Table 95. Acceptance tests of the “Assign IoT device to application user” use case 117
 Table 96. Acceptance tests of the “Log custom application event” use case..... 118
 Table 97. Acceptance tests of the “Send medical data securely” use case 118
 Table 98. Acceptance tests of the “Report suspicious activity” use case..... 119
 Table 99. Acceptance tests of the “Respond to alert” use case 119
 Table 100. Acceptance tests of the “Review alerts” use case 119
 Table 101. Acceptance tests of the “Review new risk evaluation” use case..... 120
 Table 102. Acceptance tests of the “Reflect infrastructure changes” use case 120
 Table 103. Questions and Objectives 122
 Table 104. Metrics to evaluate the situational awareness 124
 Table 105. Metrics to evaluate risk detection and mitigation 126
 Table 106. Metrics to evaluate end-to-end data protection..... 128
 Table 107. Use cases that are going to be tested during the usability test..... 133

Table of Acronyms and Definitions

| Acronym | Definition |
|---------|---|
| AI | Artificial Intelligence |
| ASQ | After-Scenario Questionnaire |
| BMI | Body Mass Index |
| BYOD | Bring Your Own Device |
| CIO | Chief Information Officer |
| ECG | Electrocardiogram |
| EHR | Electronic Health Record |
| HIS | Health Information System |
| IoT | Internet of Things |
| IT | Information Technology |
| KPI | Key Performance Indicator |
| PNP | Personalized Nutrition Plan |
| SUS | System Usability Scale |
| SIEM | Security Information and Event Management |
| SSM | System Security Modeller |
| VPN | Virtual Private Network |

I. Business Requirements

Business requirements describe the business need that leads to a novel solution capable of delivering the desired business impact [16]. In this section, we detail the business requirements of the ProTego project. Specifically, we first provide some background on the topic of cybersecurity in healthcare as a way to articulate the business problem. From that, we derive the list of project objectives. To understand how they contribute towards solving the problem, we analyze the expected impact of each, and discuss what indicators to use in order to measure success in a quantitative fashion. After that, we comment on the different stakeholders of the project and finally discuss the possible risks related to the availability (or lack thereof) of enabling technologies.

I.1. Background

The adoption of new technologies is transforming the way the healthcare sector treats people. Telemedicine, Electronic Health Records (EHR), wearables that monitor biometrics are just a few examples of what hospitals are providing as new tools to improve patients' treatment ([1], [4]).

If these transformations are contributing to enhancing the patients' health and wellbeing, they are unfortunately also increasing patients' exposure to cyber risk. In addition to giving an attacker access to health services and medical prescriptions, stolen medical data might also be instrumental in opening bank accounts, procuring passports and even getting loans [4]. Risk is further increased by the fact that, unlike credit card information, health data cannot be changed once stolen. As a result, health data are considered fifty times more valuable than financial information on the black market [5], and therefore among the most targeted kind of data [6]. As a matter of fact, it has been noticed that data breaches are becoming more and more frequent in the healthcare sector [3]. In this regard, the situation is aggravated by the fact that new trends, such as the Internet of Things (IoT) and the Bring Your Own Device (BYOD) approach, are introducing new attack vectors to healthcare institutions [2]. Recurring data breaches might have an impact on patients' trust, who might start putting in question the reliability of the healthcare sector in its ability to protect personal health records [4].

Still, compared to other organizations, the healthcare sector plods along in defending their systems [3]. Hospitals are not adopting as many defense tools as other industries. For example, in the United States, only 70% of hospital boards include cybersecurity in their risk management oversight, and only 37% of hospitals perform annual incident response exercises [9]. Evidence suggests that 39% of the healthcare organizations perform vulnerability scanning compared to the 49% of other institutions [10]. It is interesting to note that, despite the above-mentioned, the perception of having an effective threat detection system is higher in the healthcare sector than in other industries [10].

I.2. Objectives

The previous section makes it apparent that hospitals and healthcare organizations should consider the protection of medical data a priority. We can express this need in terms of the following mission statement:

“To address cybersecurity risk in healthcare”

Such a project mission can further be decomposed in various, more fine-grained project objectives. In turn – in order to successfully address cybersecurity risks, healthcare organizations should strive:

“To improve situational awareness during an attack”

“To analyze and mitigate cybersecurity risk at design-time”

“To ensure end-to-end data protection”

“To educate users on cybersecurity risk”

The success of achieving each objective is measured by means of a number of metrics, which have been identified and reported in VIII.

We believe the positive impact on healthcare organizations to be threefold. In particular, healthcare organizations would benefit from:

“Improved security of their services, data and infrastructure”

“Reduced risk of data privacy breaches”

“Increased patient trust and safety”

Figure 1 depicts the project *objectives-impacts-indicators* triad. Its purpose is to summarize at a glance what the toolkit is intended to do and how success is going to be measured. It also reports the features that are going to be implemented in order to enable the target objectives. In this matter, note that the objective of educating users to cybersecurity risk is not associated with any technical feature, focusing instead on methodologies and processes. A more in-depth discussion on the features comprising the ProTego toolkit is presented in Section II.

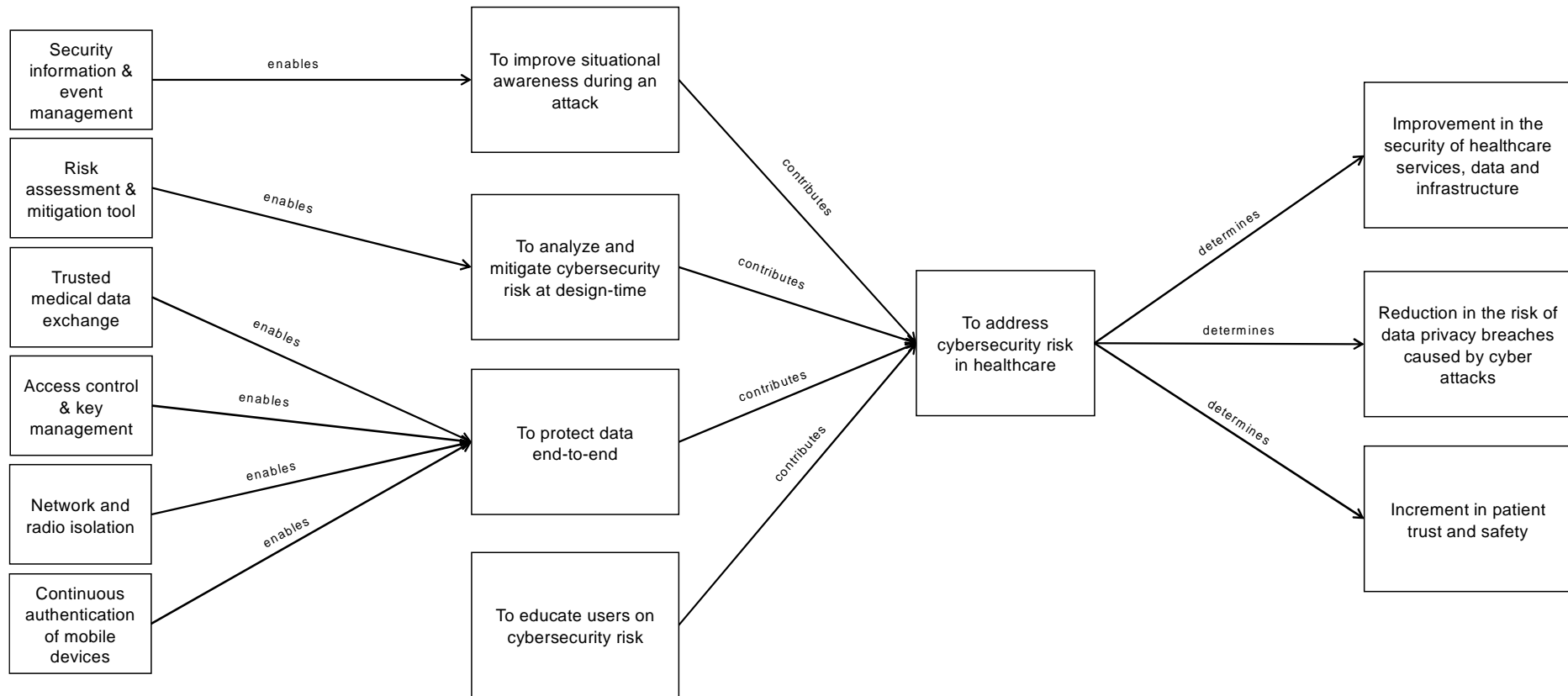


Figure 1. The relationship between objectives, the features enabling them and their impact

I.3. Stakeholders

Stakeholder analysis aims at answering the question “*who is the project for?*”. In this regard, a convenient method for organizing the analysis of stakeholders and depicting at once all interested parties is to construct a *Stakeholder map* ([10], [12]). A stakeholder map is an onion diagram meant to report fundamental socio-technical information regarding the system under development. The specific stakeholder map of the ProTego toolkit is reported in Figure 2.

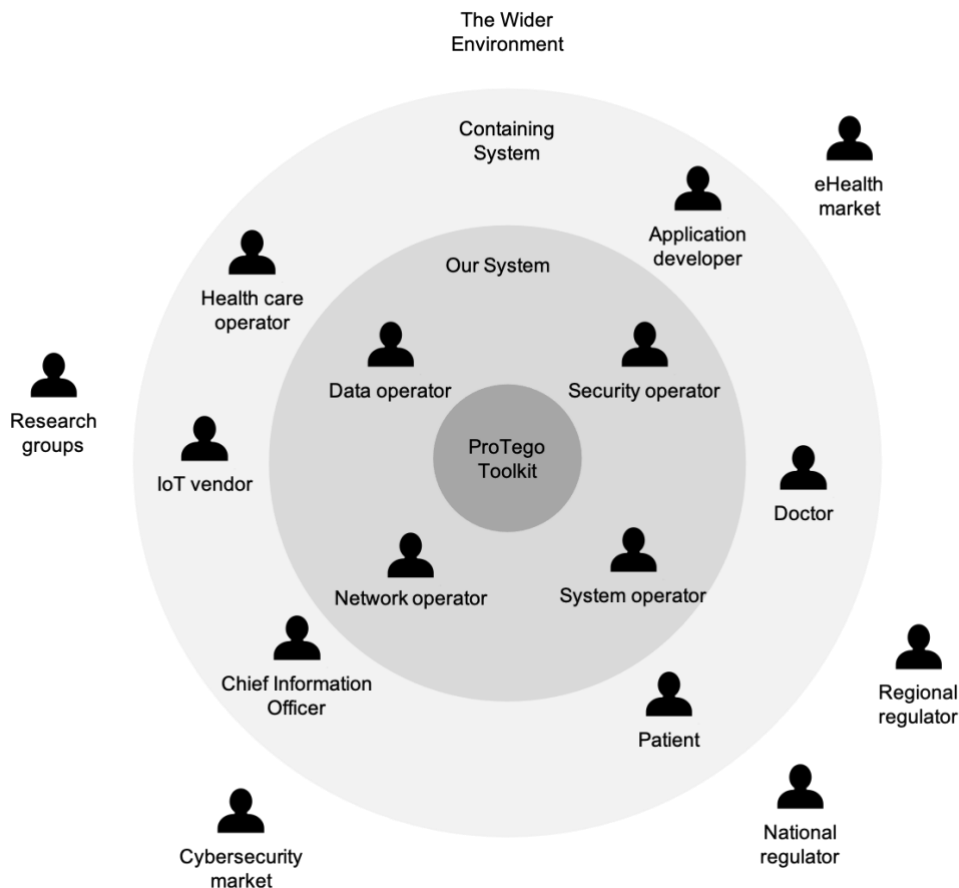


Figure 2. Stakeholder map of the ProTego toolkit

As with any complex system, the ProTego toolkit consists of a set of interrelated components working together towards a common goal [13]. In a sense, such interacting components also include the people operating such a system. They are the network, security, system and data operators running the ProTego software solution within the hospital infrastructure. We consider them as part of the system under development and address them as the direct stakeholders of the ProTego toolkit.

The ProTego toolkit is meant to be part of a greater system, i.e., the hospital as a whole. As a matter of fact, several groups of actors working in the hospital benefit from the availability of the ProTego solution. Such groups include doctors, patients and healthcare operators in general. Their day-to-day activity is directly affected by the presence of the system, making them the *functional beneficiaries* of the ProTego toolkit. Expectedly, the Chief Information Officer (CIO) is also included among the beneficiaries. Note that application developers working in the eHealth sector are likewise part of this group, as they can develop their applications by taking advantage of the software facilities provided by the ProTego toolkit. Examples of interacting systems are reported in Section V (Nutritional case study) and Section VI (Electronic Health Record case study). Similarly, IoT vendor operating in the eHealth sector may be interested in developing devices capable of interacting with ProTego-powered infrastructures.

Finally, the wider environment includes indirect stakeholders. These are research groups, regional and national regulators, along with the cybersecurity and eHealth market.

I.4. Risks

At the time of D2.2-V2, we reported that with the establishment of relevant real-life situations (see Section VII), we identified one additional relevant risk, related to IoT devices. More specifically, we mentioned that off-the-shelf IoT devices would not provide enough personalization to be adapted to the ProTego technology solution.

As this was the case, the consortium took care of developing a prototypal IoT device with representative characteristics. As mentioned in the mission statement, ProTego is concerned with the problem of addressing cybersecurity risks in healthcare, rather than creating IoT devices for healthcare. A representative, if prototype, IoT device can contribute to the project mission by providing the required supporting elements for the validation of the project case studies without distracting the consortium from its core project objectives.

II. Scope

In this section, we determine the scope of the final release of ProTego, that is, the set of functionalities that will ultimately be part of the solution. We do so by first reiterating on the set of major features of the toolkit, as also presented during its first release, and then detailing the exact rendition of each of them in the final version of the toolkit.

II.1. Features

A feature is an area of functionality that a solution should ultimately include in order to meet the project objectives. Table 1 reports the six major features comprising the ProTego toolkit.

Table 1. Major features of the ProTego toolkit

| Feature | Description |
|---|--|
| Trusted medical data exchange | The capability of the hospital to exchange data while preserving their protection in use, in transfer and at rest |
| Mobile device security | The capability of detecting suspicious activity from mobile endpoints and consequently reacting accordingly in case of threats |
| Network and radio slicing | The capability of abstracting network resources from physical elements, isolating network traffic and devoting capacity to certain purposes as needed |
| Access control & key management | The capability of controlling access to the medical data stored within the healthcare infrastructure |
| Security information & event management | The capability of collecting logs, correlating them and having real-time intelligence |
| Risk assessment and mitigation | The capability of analyzing a system in order to identify potential threats, determine possible mitigation strategies, and rapidly reanalyzing it in response to changes |

II.2. Final Release

An effective way of communicating what is going to be part of a release is to make use of a *Feature tree*. A feature tree is a fishbone diagram that shows the organization of the features in logical groups, displaying at once the scope of a solution ([15], [16]). The feature tree of the final release the ProTego toolkit is presented in Figure 3. The horizontal line represents the solution being implemented. Each branch stemming from it represents a Level 1 feature, that is, a major feature of the toolkit. In turn, each such feature may consist of Level 2 features. In the same way, a given Level 2 feature may decompose in a number of Level 3 features. For instance, the “Network and radio slicing” feature includes the capability of carrying out management activities, such as setting up new network slices.

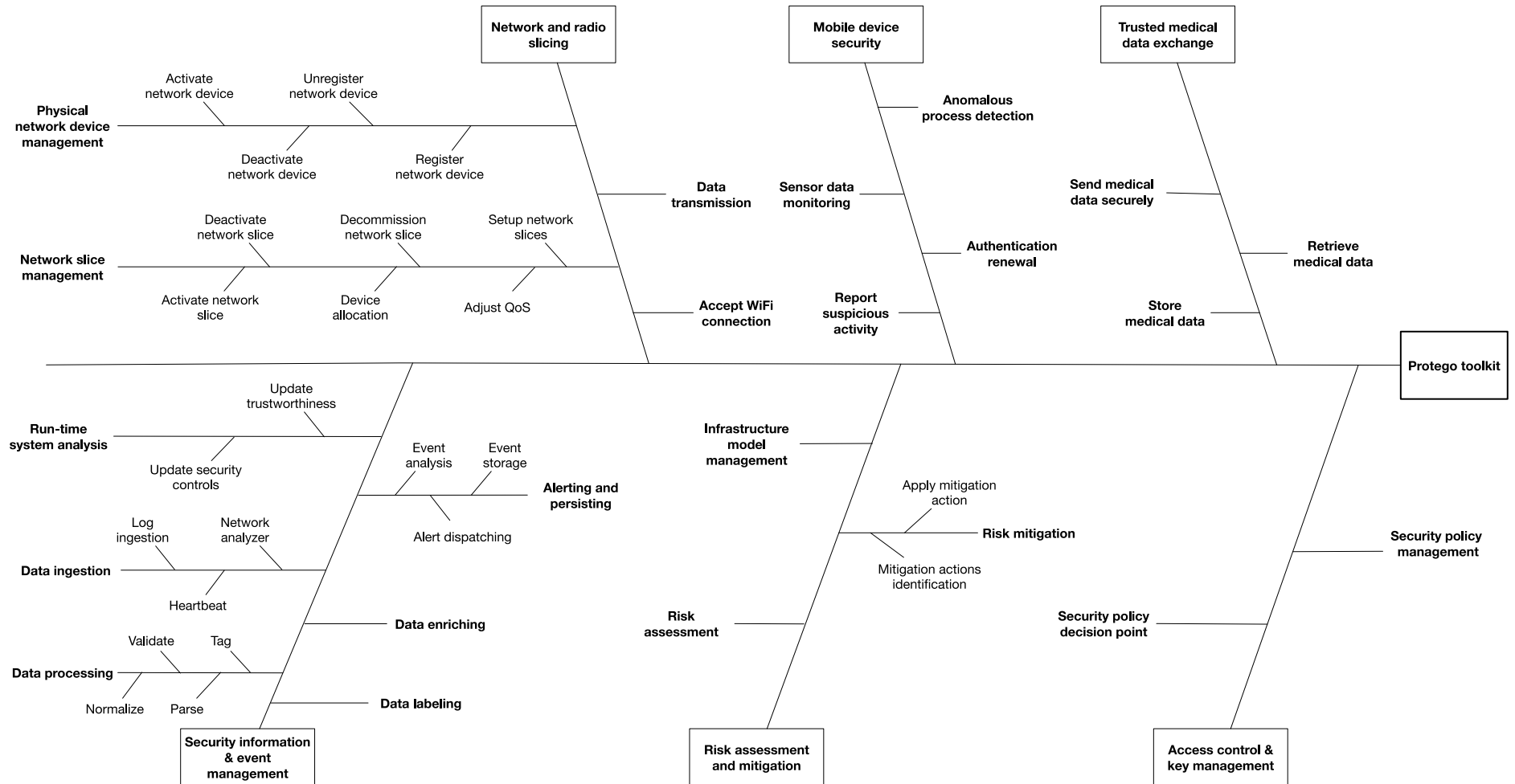


Figure 3. Feature tree of the ProTego toolkit

III. User Requirements

User requirements describe goals and tasks that specific classes of users must be able to perform with the system [16]. In order to identify the user requirements of ProTego, we begin with the presentation of its user personas. Then, we identify the user roles of interest for the ProTego toolkit. After that, we illustrate the main scenarios of interaction with the toolkit by means of a storyboard. User requirements are finally reported in the form of use cases, an effective way of detailing how different roles interact with the system, and to what end.

III.1. Personas

A *Persona* is an imaginary and yet archetypical user for whom the solution is built [18]. Specifying requirements for personas, rather than generic users, helps reduce elasticity, that is, the (unfounded) ability of the user to accommodate whatever assumption the stakeholders make about him [19]. By narrowing their variety, the resulting solution can focus on supporting only the specific users for which it was built. In the case of ProTego, development should focus on providing what is best for Carlo, as described in Table 2, and Andrew, as described in Table 3, in accordance with their skills, motivations and goals.

Table 2. Carlo, the “Network operator” persona


| | |
|--|---|
|  <p><i>“I guarantee the availability of the hospital infrastructure”</i></p> | |
| User role | Network operator |
| Description | Carlo, 38 years old. He works as a network operator in the IT department of the hospital. He is in charge of installing configuring and maintaining the network components within the hospital infrastructure. His primary duty is to monitor and analyze the network, eventually resolving network issues in order to maximize uptime. As part of his job, Carlo performs technical research on network upgrades to address short-, mid- and long-term necessities. |
| Goals | His goal is to collaborate with the other technical staff to ensure connectivity, compatibility and availability of the system. |
| Needs & opportunity | He needs to uphold confidentiality when it comes to information regarding the networks |

Table 3. Andrew, the “IT infrastructure manager” persona

| | |
|---|--|
|  <p><i>“I manage the functioning and security of the hospital’s IT infrastructure”</i></p> | |
| User role | IT infrastructure manager |
| Description | <p>Andrew, 45 years old. He works as an IT infrastructure manager in the hospital IT department.</p> <p>He is responsible for planning, managing and designing the IT infrastructure and coordinating the team responsible for maintaining this infrastructure. Given the nature of his work, he is able to effortlessly assume a technical or managerial role. Indeed, almost every task in which the IT department team is involved, from performing routine system updates to the installation of new components, is executed under his supervision. In parallel, he collaborates with colleagues and heads of other departments in order to develop strategies that will help his team better align with the company's overall strategy.</p> <p>Passionate about his work, in his spare time he devotes himself to writing technical guides on system automation and the Linux operating system.</p> |
| Goals | <p>His goal is to ensure the functioning and security of the entire IT infrastructure. By doing that, he guarantees that all data in the infrastructure are used, transmitted and stored appropriately and securely.</p> |
| Needs & opportunity | <ul style="list-style-type: none"> • He wants to integrate new applications in the hospital infrastructure • He wants to secure data in use, in transit and at rest • He wants to assess the cybersecurity associated with the infrastructure |

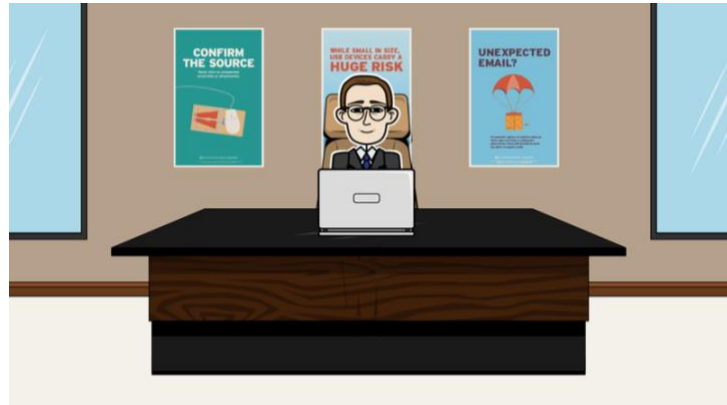
III.2. Storyboard

A *Storyboard* is a series of continuing panels, sketches, or scenes depicting a plot or sequence of actions [20]. With their combination of drawing and words, storyboards are valuable tools for exploring scenarios, which can be later generalized to use cases. For this reason, storyboards are mostly useful for illustrative purposes, without the specific intent of detailing how each situation will be implemented. In Table 4, we report the storyboard for ProTego. The storyboard focuses the installation process of FoodCoach, the demonstration platform for the Nutritional case study of Section V. An analogous process applies for the EHR case study of Section VI.

Table 4. Storyboard between stakeholders, as mediated by ProTego

Step 1

Steve, the hospital CIO, wants to adopt a new infrastructure technology capable of meeting the ever-increasing needs of the hospital



Step 2

To this end, he asks his IT team to install ProTego as the infrastructure solution for the hospital



Step 3

Andrew starts the installation process



Step 4

As part of the installation process, Andrew sets the admin password for ProTego

```
<?xml version="1.0" encoding="UTF-8"?>
<protego-configuration>
  <!-- many other configurations -->
  <root password="protegomaxima" />
</protego-configuration>
```

Step 5

Logged as System Operator, Andrew deploys the cluster for ProTego

```
$ ./install-cluster.sh
$ add-node -u andrew -host 192.168.25.1
andrew's password:
$ add-node -u andrew -host 192.168.25.2
andrew's password:
$ add-node -u andrew -host 192.168.25.3
andrew's password:
$
```

Step 6

Logged as System Operator, Andrew installs the Data Gateway

```
$ ./install-datagateway.sh
andrew's password:
$
```

Step 7

Logged as System Operator,
Andrew installs the Network
Slicing

```
$ ./install-networkslicing.sh  
andrew's password:  
$
```

Step 8

Logged as System Operator,
Andrew installs the SIEM

```
$ ./install-SIEM.sh  
andrew's password:  
$
```

Step 9

Logged as System Operator,
Andrew installs the SSM

```
$ ./install-SSM.sh  
andrew's password:  
$
```

Step 10

Logged as System Operator, Andrew installs Continuous authentication

```
$ ./install-continuousauthentication.sh
andrew's password:
$
```

Step 11

For each component, Andrew adds authorized users

```
$ network-slicing -u add user andrew -r *,!network-operator
root's password:
user "andrew" created
$ network-slicing -u root add user carlo -r network-operator
root's password:
user "carlo" created
$
```

Step 12

Andrew tells Steve that ProTego is now up and running in the hospital



Step 13

Andrew maps and assesses the hospital infrastructure using the graphical editor of ProTego.



Step 14

Steve meets with Elisa, a nutritionist of the hospital, and they discuss the needs of the nutrition department



Step 15

Steve organizes a meeting with Elisa, Andrew and Anna, a representative of FoodCoach



Step 16

Andrew assesses the potential impact of FoodCoach on the infrastructure using the graphical editor of ProTego



Step 17

Eventually, FoodCoach is adopted by OSR



Step 18

Anna provides the hospital with the necessary specifications for integrating FoodCoach



Step 19

Logged as System Operator, Andrew proceeds with the installation of FoodCoach

```
$ ./install-foodcoach.sh
```

Step 20

Logged as Network Operator, Carlo configures the application network slices

```
$ protego \  
-u carlo config foodcoach slices -f foodcoach.slices  
carlo's password:  
$
```

Step 21

As a part of the network configuration, Elisa goes to the IT department to have her mobile device registered in the system

```
$ protego \  
-u carlo assign foodcoach mobile 87:4f:41:63:6e:4b \  
--owner elisa@hsr.it \  
--slices nutritionist-slice  
carlo's password:  
$
```

Step 22

Logged as Security Operator, Andrew configures the application logging mechanism

```
$ protego \  
-u andrew config foodcoach logging -f foodcoach.logging  
andrew's password:  
$
```

Step 23

Logged as Security Operator, Andrew specifies the application access control

```
$ protego \  
-u andrew config foodcoach acontrol -f foodcoach.acontrol  
andrew's password:  
$
```

Step 24

Logged as Security Operator, Andrew populates the application with its initial medical data

```
$ protego \  
-u andrew create foodcoach med-data -f foodcoach.mdata  
andrew's password:  
$
```

Step 25

In the meantime, Elisa brings her smartphone to the IT department



Step 26

Andrew configures continuous authentication agent on Elisa's mobile device



Step 27

IT department returns the device to Elisa



Step 28

In the meantime, Andrew notifies Manuel, the FoodCoach admin, that FoodCoach is ready to be used



Step 29

Manuel setups the accounts for the nutritionists via FoodCoach



Step 30

Elisa meets Antonella, one of her new patients



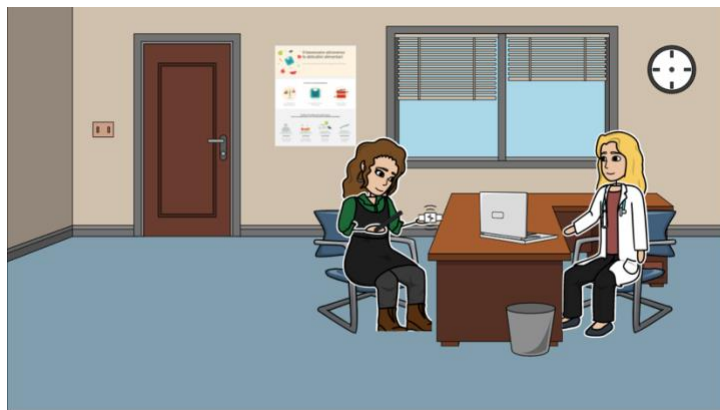
Step 31

Elisa delivers the device to Antonella



Step 32

Antonella provides the application credentials, and she is associated with that device



Step 33

Elisa uses FoodCoach in her daily activities with her desktop computer...



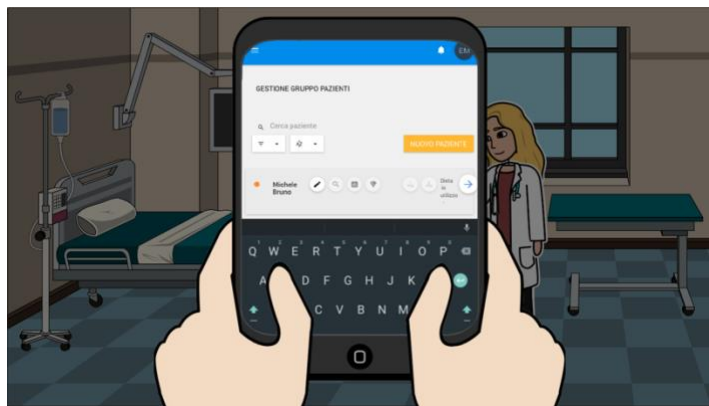
Step 34

...while taking advantage of network slicing for the time she uses FoodCoach in mobility, within the hospital premises



Step 35

After an initial period of training, the system is able to recognize Elisa's behavioral pattern, which enables a number of mobile security measures



Step 36

After collecting enough information, the system determines a baseline of normal behavior. From that, the system is able to identify run-time anomalies and consequently notify Andrew



Step 37

While operating, the hospital is subject to a number of attacks



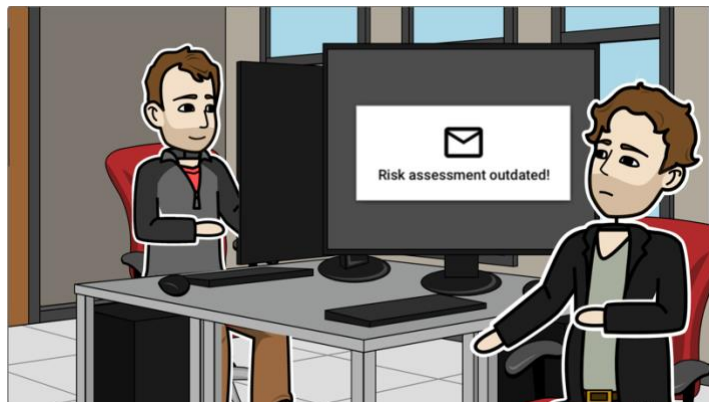
Step 38

Every time ProTego detects an attack, it sends an alert to Andrew, so that he is able to put in place relevant mitigation strategies



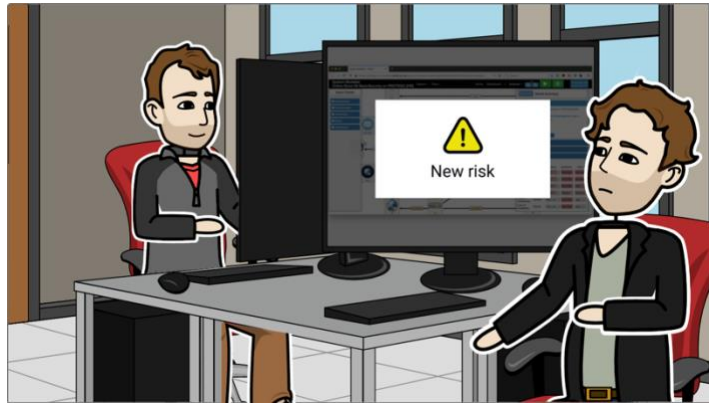
Step 39

Through the use of artificial intelligence, the system continuously updates its evaluations



Step 40

As a result, Andrew may be notified that the system identified new risks even if no infrastructural change took place



Step 41

When this happens, Andrew puts in place relevant mitigation strategies



III.3. Roles

Users of the ProTego toolkit may be distinguished by the role they play with respect to the system. In this regard, the user roles in Table 5 directly stem from the direct stakeholders, that is, stakeholders that are part of the inner ring in the Stakeholder map of Section I.3.

Table 5. User roles of the ProTego toolkit

| User role | Description |
|-------------------|---|
| Network operator | Network operators manage the network capabilities of the hospital. They need to guarantee that the network meets the necessary quality of service attributes |
| Data operator | Data operators are in charge of data flows and how they are stored within the hospital infrastructure. Data operators must guarantee that sensitive data are stored with an appropriate level of protection |
| Security operator | Security operators take care of the security concerns of the hospital infrastructure. These include controlling access to the hospital services, assessing the risk associated with the infrastructure, and monitoring the data exchange for possible attacks and foreseeable risks |
| System operator | System operators are responsible for installing, configuring and managing computer systems in the hospital infrastructure |
| Administrator | Special role capable of making unrestricted, system-wide changes (e.g., registering accounts for other IT operators) |
| Application | Third-party applications providing some service in the context of the hospital. Applications interact with the ProTego toolkit via a computerized public interface |
| IoT device | An embedded system, equipped with sensors and capable of transmitting data over a network without human intervention |
| Mobile agent | Mobile software service capable of automatically informing the ProTego environment of relevant events occurring in a mobile device |

In addition to those, we also have *interacting systems*, which communicate with the ProTego toolkit by means of, e.g., some application-to-application interface (such as REST). These are the Nutritional application of Section V and the EHR application of Section VI, as well as the IoT and Mobile devices in use at the hospital. Since the ProTego toolkit provides a service to such interacting systems, they should also be codified as a user role of the ProTego toolkit [14]. These roles appear as *Application*, *IoT device* and *Mobile agent* in Table 5.

III.4. Use cases

Use cases are descriptions of a set of logically related interactions between an actor and a system that results in an outcome that provides value to the actor [16]. The use cases diagram in Figure 4 reports the expected use cases of the ProTego toolkit. In this regard, it should be noted that the proposed use cases are *sea-level* use cases, that is, use cases that address the question "Can the primary actor go away happy after having done this?" [17]. In contrast, we omitted lower-level use cases such as "Log into the platform", which hardly represent the real user goal. Such core use cases are organized according to a well-established template ([16], [14]), starting from Table 7 to Table 31

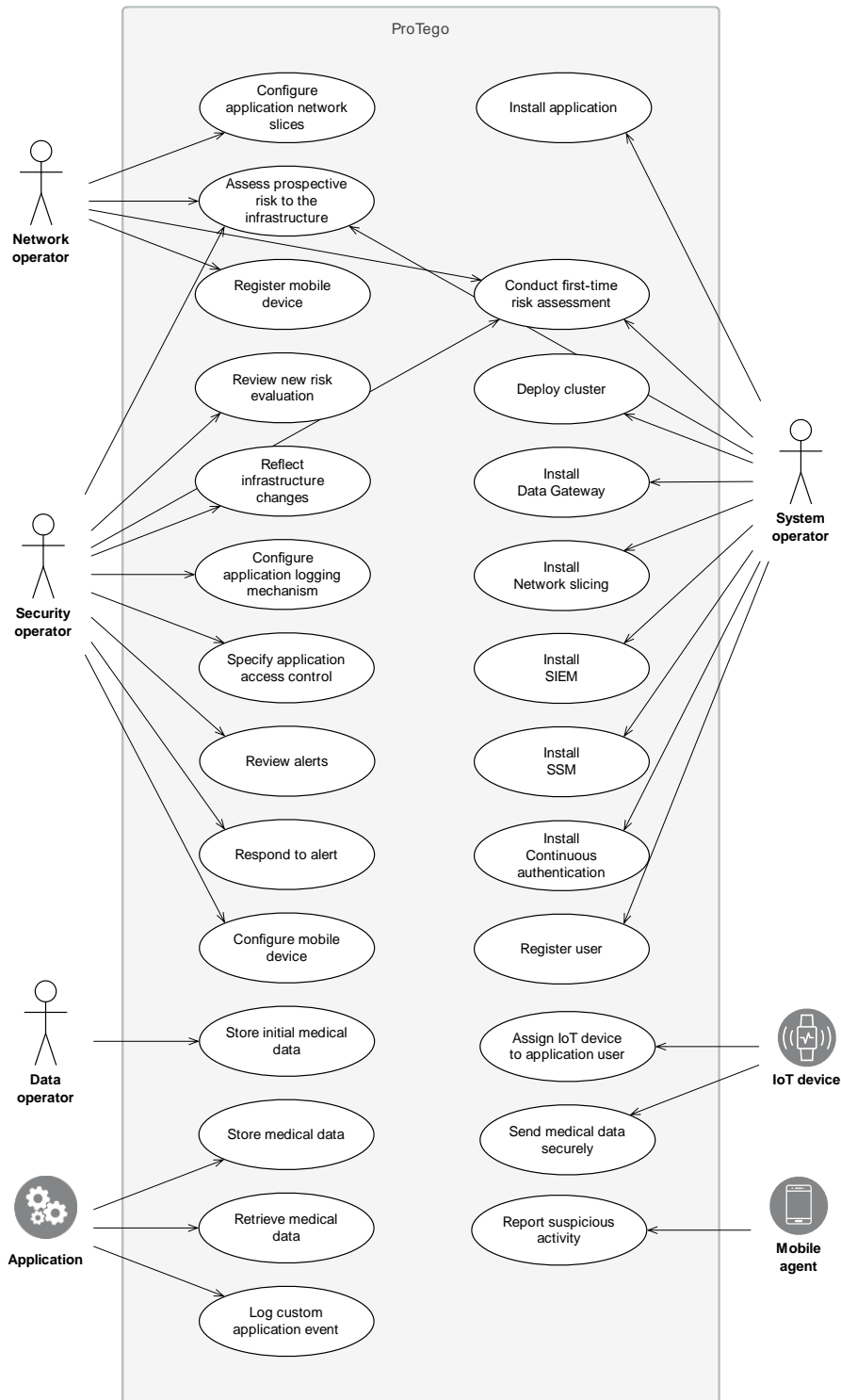


Figure 4. Use case diagram of the ProTego toolkit

Table 6. “Deploy cluster” use case

| | |
|----------------------|---|
| Identifier | UC01 |
| Goal | Deploy cluster |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | 1. System Operator account has been set up and enabled |
| Success guarantee | 1. The cluster is deployed in the hospital and the components of the ProTego Toolkit are ready to be installed |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator sets up the required virtual machines 3. System Operator configures a master node and the required worker nodes 4. System Operator uses the configured nodes to set up a cluster 5. The cluster is deployed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 7. “Install Data Gateway” use case

| | |
|----------------------|---|
| Identifier | UC02 |
| Goal | Install Data Gateway |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | <ol style="list-style-type: none"> 1. The cluster is deployed in the hospital 2. System Operator account has been set up and enabled |
| Success guarantee | 1. The Data Gateway is installed in the hospital premises |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator deploys the FHIR server 3. System Operator deploys the Query Gateway 4. System Operator deploys the Access Control framework 5. Data Gateway is installed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 8. “Install Network Slicing” use case

| | |
|----------------------|---|
| Identifier | UC03 |
| Goal | Install Network Slicing |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | <ol style="list-style-type: none"> 1. The cluster is deployed in the hospital 2. System Operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. The Network Slicing is installed in the hospital premises |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator deploys the Network Slicing controller 3. System Operator installs the access point 4. System Operator registers the access point in the Network Slicing controller 5. Network Slicing is installed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 4. System reports error: “Unauthorized” 5. System logs the unsuccessful attempt access 6. System terminates the use case <p>E2. Access Point has already been registered</p> <ol style="list-style-type: none"> 4. System reports error: “Access point has already been registered” 5. System terminates the use case |

Table 9. “Install SIEM” use case

| | |
|----------------------|--|
| Identifier | UC04 |
| Goal | Install SIEM |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | <ol style="list-style-type: none"> 1. The cluster is deployed in the hospital 2. System Operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. The SIEM agent is installed in the hospital premises 2. The SIEM log analyzer is installed in the hospital premises |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator asks to deploy the SIEM log analyzer 3. System Operator asks to deploy the SIEM agent 4. System Operator configures a mechanism to redirect logs from the application to the SIEM agent 5. The SIEM is installed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt access 3. System terminates the use case |

Table 10. "Install SSM" use case

| | |
|-----------------------------|---|
| Identifier | UC05 |
| Goal | Install SSM |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | <ol style="list-style-type: none"> 1. The cluster is deployed in the hospital 2. System Operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. The SSM is installed in the hospital premises |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator asks to deploy the SSM 3. The SSM is installed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: "Unauthorized" 2. System logs the unsuccessful attempt access 3. System terminates the use case |

Table 11. "Install Continuous authentication" use case

| | |
|-----------------------------|--|
| Identifier | UC06 |
| Goal | Install Continuous authentication |
| Actor | System Operator |
| Trigger | The ProTego Toolkit has been adopted to be used in the hospital |
| Precondition | <ol style="list-style-type: none"> 1. The cluster is deployed in the hospital 2. System Operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. The Continuous Authentication is installed in the hospital premises |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator asks to deploy the EDR component 3. System Operator asks to deploy the JBCA component 4. The Continuous Authentication is installed in the hospital |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: "Unauthorized" 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 12. “Register user in a component” use case

| | |
|----------------------|---|
| Identifier | UC07 |
| Goal | Register user |
| Actor | System Operator |
| Trigger | A new operator is assigned to the management of the component |
| Precondition | 1. System Operator account has been set up and enabled |
| Minimal guarantee | 1. The outcome and details of the operation are logged as an event |
| Success guarantee | 1. The new user is registered in the component |
| Success scenario | <ol style="list-style-type: none"> 1. System Operator logs into his account 2. System Operator asks to register a new user 3. System Operator specifies the name and associated roles of the new user 4. System registers the indicated user and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case <p>E2. User identifier already taken</p> <ol style="list-style-type: none"> 5. System reports error: “User identifier already taken” 6. System logs the unsuccessful attempt as an event 7. System terminates the use case |

Table 13. “Conduct first-time risk assessment” use case

| | |
|----------------------|---|
| Identifier | UC08 |
| Goal | Conduct first-time risk assessment |
| Actor | Security operator |
| Supporting actors | System operator, Network operator |
| Trigger | The system is adopted as the infrastructure solution for the hospital |
| Precondition | <ol style="list-style-type: none"> 1. Risks to the infrastructure are still to be assessed 2. Security operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. The infrastructure is modeled into the system 2. The risks associated with the infrastructure are assessed 3. The details of the operation are logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security operator logs into his account 2. Security operator asks to assess the risks to the infrastructure 3. With the assistance of System and Network operator, Security operator provides the infrastructure model mapping the hospital infrastructure 4. System stores the infrastructure model 5. System displays risks and mitigation actions, and logs the operation as an event |
| Exceptional scenario | E1. Insufficient authorization |

| | |
|--|--|
| | <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt access 3. System terminates the use case <p>E2. First-time assessment already conducted</p> <ol style="list-style-type: none"> 4. System reports error: “Already existing model” 5. System logs the unsuccessful attempt 6. System terminates the use case |
|--|--|

Table 14. “Assess prospective risks to the infrastructure” use case

| | |
|-----------------------------|---|
| Identifier | UC09 |
| Goal | Assess prospective risks to the infrastructure |
| Actor | Security operator |
| Supporting actors | System operator, Network operator |
| Trigger | The IT operators are considering a change to the infrastructure (e.g., because of a new application) |
| Precondition | <ol style="list-style-type: none"> 1. The infrastructure has been modeled into the system 2. Security operator account has been set up and enabled |
| Success guarantee | <ol style="list-style-type: none"> 1. Prospective risks to the infrastructure are assessed 2. The details of the operation are logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security operator logs into his account 2. Security operator asks to assess the prospective risks to the infrastructure 3. With the assistance of System and Network operator, Security operator provides an infrastructure model that includes the changes under consideration 4. System computes and displays risks and mitigation actions, and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt access 3. System terminates the use case <p>E2. Prospective risk assessment already conducted</p> <ol style="list-style-type: none"> 1. System reports error: “Already existing model” 2. System logs the unsuccessful attempt 3. System terminates the use case |

Table 15. "Install application" use case

| | |
|-----------------------------|---|
| Identifier | UC10 |
| Goal | Install application |
| Actor | System operator |
| Trigger | An application has been approved for integration in the infrastructure |
| Precondition | 1. System operator account has been set up and enabled |
| Minimal guarantee | 1. The outcome and details of the operation are logged as an event |
| Success guarantee | 1. Application is installed in the system |
| Success scenario | <ol style="list-style-type: none"> 1. System operator logs into his account 2. System operator asks to install the application 3. The system installs the application and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 2. System reports error: "Unauthorized" 3. System logs the unsuccessful attempt to access 4. System terminates the use case <p>E2. Application already installed</p> <ol style="list-style-type: none"> 2. System reports error: "Application already installed" 3. System logs the unsuccessful attempt as an event 4. System terminates the use case |

Table 16. "Configure application network slices" use case

| | |
|-----------------------------|---|
| Identifier | UC11 |
| Goal | Configure application network slices |
| Actor | Network operator |
| Trigger | An application has been approved for integration in the infrastructure |
| Precondition | <ol style="list-style-type: none"> 1. Network operator account has been set up and enabled 2. Application is installed in the system 3. Application network slices are still to be configured |
| Minimal guarantee | <ol style="list-style-type: none"> 1. The outcome and details of the operation are logged as an event |
| Success guarantee | <ol style="list-style-type: none"> 1. Application network slices are configured |
| Success scenario | <ol style="list-style-type: none"> 1. Network operator logs into his account 2. Network operator asks to configure network slices 3. Network operator specifies the names of the network slices and their quality-of-service attributes and the traffic configuration 4. System creates the network slices, and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 3. System reports error: "Unauthorized" 4. System logs the unsuccessful attempt to access 5. System terminates the use case <p>E2. Network slices are already configured</p> <ol style="list-style-type: none"> 3. System reports error: "Network slices are already configured" 4. System logs the unsuccessful attempt to access 5. System terminates the use case |

Table 17. “Configure application logging mechanism” use case

| | |
|-----------------------------|---|
| Identifier | UC12 |
| Goal | Configure application logging mechanism |
| Actor | Security operator |
| Trigger | A new application has been registered in the system |
| Precondition | <ol style="list-style-type: none"> 1. Security operator account has been set up and enabled 2. Application is installed in the system 3. Application logging mechanism is still to be configured |
| Success guarantee | <ol style="list-style-type: none"> 1. Application logging mechanism is configured 2. The operation is logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security operator logs into his account 2. Security operator asks to configure application logging mechanism 3. Security operator specifies the application event sources 4. Security operator specifies – for each source, the corresponding processing strategy, and possible enriching information 5. Security operator specifies the application correlation rules and statistical models associated with the application events 6. System puts in place the application logging mechanism and logs the operation as an event |
| Alternative scenario | <p>A1. The application uses additional event sources</p> <ol style="list-style-type: none"> 3a. Security operator specifies additional event sources |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 18. “Specify application access control” use case

| | |
|----------------------|--|
| Identifier | UC13 |
| Goal | Specify application access control |
| Actor | Security operator |
| Trigger | A new application has been installed in the system |
| Precondition | <ol style="list-style-type: none"> 1. Security operator account has been set up and enabled 2. Application is installed in the system 3. Application access control is still to be configured |
| Success guarantee | <ol style="list-style-type: none"> 1. Application access control is active 2. The operation is logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security operator logs into his account 2. Security operator asks to specify access control 3. Security operator supplies the access control specification (i.e., roles and permissions) associated with the application 4. System activates the indicated access control specification and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 19. “Configure mobile device” use case

| | |
|----------------------|--|
| Identifier | UC14 |
| Goal | Configure mobile device |
| Actor | Security operator |
| Trigger | A new application needs to be used on the mobile device |
| Precondition | <ol style="list-style-type: none"> 1. The continuous authentication component has been installed in the system 2. Application is installed in the system 3. The continuous authentication agent is still to be configured |
| Success guarantee | <ol style="list-style-type: none"> 1. Continuous authentication agent is active 2. The operation is logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security operator asks to configure continuous authentication agent 2. Security operator provides the necessary configuration details 3. The continuous authentication agent is activated |
| Exceptional scenario | <p>E1. Mobile device already configured</p> <ol style="list-style-type: none"> 4. The agent reports error: “Mobile device is already configured” 3. The agent terminates the use case |

Table 20. “Store initial medical data” use case

| | |
|-----------------------------|---|
| Identifier | UC15 |
| Goal | Store initial medical data |
| Actor | Data operator |
| Trigger | A new application has been registered in the system |
| Precondition | <ol style="list-style-type: none"> 1. Data operator account has been set up and enabled 2. Application is installed in the system 3. The initial medical data of an application are still to be stored |
| Success guarantee | <ol style="list-style-type: none"> 1. The initial medical data of an application are stored in the system 2. The operation is logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Data operator logs into his account 2. Data operator asks to store the initial medical data of an application 3. Data operator uploads the initial medical data 4. System stores the medical data and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case <p>E2. Application initial resources are already stored</p> <ol style="list-style-type: none"> 3. System reports error: “Initial resources already stored” 4. System logs the unsuccessful attempt to access 5. System terminates the use case |

Table 21. “Register mobile device” use case

| | |
|-----------------------------|---|
| Identifier | UC16 |
| Goal | Register mobile device |
| Actor | Network operator |
| Trigger | Application user wants to access the application in mobility inside the hospital premises |
| Precondition | <ol style="list-style-type: none"> 1. Network operator account has been set up and enabled 2. Application is installed in the system 3. The network slicing controller is configured |
| Minimal guarantee | <ol style="list-style-type: none"> 1. The outcome and details of the operation are logged as an event |
| Success guarantee | <ol style="list-style-type: none"> 1. Mobile device is registered in the system |
| Success scenario | <ol style="list-style-type: none"> 1. Network operator logs into his account 2. Network operator asks to register a new mobile device 3. Network operator specifies the device identifier 4. System registers the mobile device, and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case <p>E2. Device already registered</p> <ol style="list-style-type: none"> 3. System reports error: “Device already registered” 4. System logs the unsuccessful attempt as an event 5. System terminates the use case |

Table 22. “Store medical data” use case

| | |
|-----------------------------|--|
| Identifier | UC17 |
| Goal | Store medical data |
| Actor | Application |
| Trigger | Application needs to store some medical data |
| Precondition | <ol style="list-style-type: none"> 1. Application is installed in the system 2. Application has obtained an authorization token on behalf of some application user |
| Minimal guarantee | <ol style="list-style-type: none"> 1. The outcome and details of the operation are logged as an application event |
| Success guarantee | <ol style="list-style-type: none"> 1. Medical data is stored in the system |
| Success scenario | <ol style="list-style-type: none"> 1. Application sends to the system the authorization token and new medical data to be stored 2. System stores the medical data and logs the operation as an application event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 2. System reports error: “Unauthorized” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E2. Authorization token is expired</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is expired” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E3. Authorization token is ill-formed</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is ill-formed” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case |

Table 23. “Retrieve medical data” use case

| | |
|-----------------------------|---|
| Identifier | UC18 |
| Goal | Retrieve medical data |
| Actor | Application |
| Trigger | Application needs to retrieve some medical data |
| Precondition | <ol style="list-style-type: none"> 1. Application is installed in the system 2. Application has obtained an authorization token on behalf of some application user |
| Minimal guarantee | <ol style="list-style-type: none"> 1. The outcome and details of the operation are logged as an application event |
| Success guarantee | <ol style="list-style-type: none"> 2. Medical data are retrieved |
| Success scenario | <ol style="list-style-type: none"> 1. Application sends to the system the authorization token together with the query of interest 2. System retrieves the requested medical data and logs the operation as an application event 3. Application receives a (possibly empty) set of medical data |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 2. System reports error: “Unauthorized” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E2. Medical data have been tampered with</p> <ol style="list-style-type: none"> 2. System reports error: “Corrupted data” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E3. Authorization token is expired</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is expired” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E4. Authorization token is ill-formed</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is ill-formed” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case |

Table 24. “Assign IoT device to application user” use case

| | |
|-----------------------------|--|
| Identifier | UC19 |
| Goal | Assign IoT device to application user |
| Actor | Application |
| Trigger | IoT device is handed to some application user |
| Precondition | <ol style="list-style-type: none"> 1. Application is installed in the system 2. IoT device has not been assigned yet 3. The user has signed up for an account on the application |
| Minimal guarantee | <ol style="list-style-type: none"> 3. The outcome and details of the operation are logged as an application event |
| Success guarantee | <ol style="list-style-type: none"> 3. The IoT device is assigned to the indicated application user |
| Success scenario | <ol style="list-style-type: none"> 1. The user gets prompted to enter his username and password to assign the IoT device to his existing Pocket EHR account 2. IoT device sends the login request to the cloud authentication system with the user and password provided 3. The IoT device successfully authenticates and receives a JWT_Token, containing both an ID_Token and a Refresh_Token 4. The IoT device stores the JWT_Token |
| Alternative scenario | <p>A1. Assign IoT device to a new user</p> <ol style="list-style-type: none"> 4. The IoT device overwrites the previous JWT_Token with the new one |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 4. System reports error: “Unauthorized” 5. System logs the unsuccessful attempt as an application event 6. System terminates the use case <p>E2. ID_Token is expired</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is expired” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case <p>E3. ID_Token is ill-formed</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is ill-formed” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case |

Table 25. “Log custom application event” use case

| | |
|-----------------------------|---|
| Identifier | UC20 |
| Goal | Log custom application event |
| Actor | Application |
| Trigger | Application has produced a custom application event to be logged |
| Precondition | 1. Application is installed in the system |
| Minimal guarantee | 1. In case of failure, the unsuccessful attempt is logged as an application event |
| Success guarantee | 2. Custom application event is logged |
| Success scenario | <ol style="list-style-type: none"> 1. Application sends to the agent the custom application event that needs to be logged 2. The agent uses an encryption key to send the events to the analyzer component 3. System logs the custom application event |
| Exceptional scenario | <p>E1. Agent key is incorrect</p> <ol style="list-style-type: none"> 2. System reports error: “Incorrect encryption key” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case |

Table 26. “Send medical data securely” use case

| | |
|-----------------------------|---|
| Identifier | UC21 |
| Goal | Send medical data securely |
| Actor | IoT device |
| Trigger | IoT device needs to send some medical data to the system |
| Precondition | 1. IoT device has been assigned to application user |
| Minimal guarantee | 1. The outcome and details of the operation are logged as an event |
| Success guarantee | 1. The medical data are sent through the secure communication channel |
| Success scenario | <ol style="list-style-type: none"> 1. The IoT device verifies whether the ID_Token is expired 2. The IoT device issues a communication request, which includes the stored JWT_Token 3. The system authorizes the request 4. The IoT send medical data securely |
| Alternative scenario | <p>A1. Expired ID_token</p> <ol style="list-style-type: none"> 2. The IoT device uses the Refresh_Token to receive a new ID_Token 3. The IoT device issues a communication request, which includes the stored JWT_Token 4. The system authorized the request 5. The IoT send medical data securely |
| Exceptional scenario | <p>E1. Authorization token is ill-formed</p> <ol style="list-style-type: none"> 2. System reports error: “Authorization token is ill-formed” 3. System logs the unsuccessful attempt as an application event 4. System terminates the use case |

Table 27. “Report suspicious activity” use case

| | |
|--------------------------|--|
| Identifier | UC22 |
| Goal | Report suspicious activity |
| Actor | Mobile agent |
| Trigger | Mobile agent detected a suspicious activity |
| Precondition | 1. The Continuous authentication is installed in the system |
| Success guarantee | 1. The suspicious activity is recorded in the system |
| Success scenario | <ol style="list-style-type: none"> 1. Mobile agent transmits the details of the suspicious activity it detected (e.g., loss of authenticity) to the system 2. System records and processes the activity report |

Table 28. “Respond to alert” use case

| | |
|-----------------------------|---|
| Identifier | UC23 |
| Goal | Respond to alert |
| Actor | Security Operator |
| Trigger | Security Operator received an alert |
| Precondition | 1. Security Operator account has been set up and enabled |
| Success guarantee | 1. Security Operator put in place an appropriate remediation action |
| Success scenario | <ol style="list-style-type: none"> 1. Security Operator logs into his account 2. Security Operator opens the alert 3. System reports the details of the alert under consideration 4. Security Operator performs an appropriate remediation action |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 29. “Review alerts” use case

| | |
|-----------------------------|---|
| Identifier | UC24 |
| Goal | Review alerts |
| Actor | Security Operator |
| Trigger | Security operator wants to review the alerts and the events that generated them |
| Precondition | 1. Security Operator account has been set up and enabled |
| Success guarantee | 1. Security Operator is provided with a visualization of alerts and associated events |
| Success scenario | 1. Security Operator logs into his account 2. Security operator asks to review the application alerts 3. System displays alerts and the application events that originated them |
| Exceptional scenario | E1. Insufficient authorization 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case |

Table 30. “Review new risk evaluation” use case

| | |
|-----------------------------|---|
| Identifier | UC25 |
| Goal | Review new risk evaluation |
| Actor | Security Operator |
| Trigger | The system notifies the security operator that its evaluation regarding risks has changed |
| Precondition | 1. Security Operator account has been set up and enabled 2. The infrastructure has been modeled into the system |
| Success guarantee | 1. Security Operator is made aware of the changes in the system evaluation regarding risks 2. The details of the operation are logged as an event |
| Success scenario | 1. Security Operator logs into his account 2. Security operator asks to see the changes in the risk assessment 3. System displays the changes in the risk assessment, and logs the operation as an event |
| Exceptional scenario | E1. Insufficient authorization 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case E2. First-time risk assessment is still to be conducted 3. System shows that the first-time risk assessment is still to be conducted 4. System terminates the use case |

Table 31. “Reflect infrastructure changes” use case

| | |
|-----------------------------|---|
| Identifier | UC26 |
| Goal | Reflect infrastructure changes |
| Actor | Security Operator |
| Supporting actor | System Operator, Network Operator |
| Trigger | There have been changes to the infrastructure |
| Precondition | <ol style="list-style-type: none"> 1. Security Operator, Network Operator, System Operator accounts have been set up and enabled 2. The infrastructure has been modeled into the system |
| Success guarantee | <ol style="list-style-type: none"> 1. The risks of the infrastructure changes are assessed 2. The details of the operation are logged as an event |
| Success scenario | <ol style="list-style-type: none"> 1. Security Operator logs into his account 2. Security Operator asks to report some changes in the infrastructure 3. With the assistance of System and Network Operator, Security operator provides the changes to the current infrastructure model 4. System integrates the differences and stores the updated infrastructure model 5. System displays changes in the risks and mitigation actions, and logs the operation as an event |
| Exceptional scenario | <p>E1. Insufficient authorization</p> <ol style="list-style-type: none"> 1. System reports error: “Unauthorized” 2. System logs the unsuccessful attempt to access 3. System terminates the use case <p>E2. First-time risk assessment is still to be conducted</p> <ol style="list-style-type: none"> 3. System shows that the first-time risk assessment is still to be conducted 4. System terminates the use case |

IV. Quality Attributes

The quality of a system is the degree to which it satisfies the stated and implied needs of its various stakeholders, and thus provides value [21]. In this section we discuss the Quality attributes we expect from the ProTego toolkit. In particular, we focus on those that are of greatest importance for the achievement of the project goals, as quality attributes can serve as the origin of system functionalities, as well as architectural and design decisions [16]. They are listed from Table 32 to Table 39 and expressed using the EARS template [23].

IV.1. Authenticity

Authenticity denotes the degree to which the identity of a subject or resource can be proved to be the one claimed [21]. The authenticity requirements of ProTego are presented in Table 32.

Table 32. Authenticity requirements

| Identifier | Requirement |
|------------|--|
| AH01 | The system shall verify the identity of its security operators before allowing them to use the system capabilities |
| AH02 | The system shall verify the identity of its data operators before allowing them to use the system capabilities |
| AH03 | The system shall verify the identity of its network operators before allowing them to use the system capabilities |
| AH04 | The system shall verify the identity of its system operators before allowing them to use the system capabilities |
| AH05 | The system shall verify the identity of the application users before allowing them to use the system capabilities |
| AH06 | The system shall verify the identity of an application before allowing it to use the system capabilities |
| AH07 | The system shall verify the identity of an IoT device before allowing it to use the system capabilities |
| AH08 | The system shall verify the authenticity of the stored infrastructural models before processing them |
| AH09 | The system shall verify the authenticity of the stored events before processing them |
| AH10 | The system shall verify the authenticity of the stored user identities before processing them |
| AH11 | The system shall verify the authenticity of the stored medical data before processing them |
| AH12 | The system shall verify the authenticity of the stored application correlation rules before processing them |
| AH13 | The system shall verify the authenticity of the stored application statistical models before processing them |
| AH14 | The system shall verify the authenticity of the stored application roles before processing them |
| AH15 | The system shall verify the authenticity of the stored application permissions before processing them |
| AH16 | The system shall verify the authenticity of the stored application details before processing them |

IV.2. Integrity

From a security standpoint, *Integrity* is concerned with inhibiting unauthorized writing [22]. More generally, integrity deals with preventing information loss and preserving the correctness of data entered into the system [16]. Table 33 contains the list of integrity requirements of ProTego.

Table 33. Integrity requirements

| Identifier | Requirement |
|------------|---|
| IN01 | The system shall prevent the unauthorized writing of infrastructure models |
| IN02 | The system shall prevent the unauthorized writing of events |
| IN03 | The system shall prevent the unauthorized writing of user identities |
| IN04 | The system shall prevent the unauthorized writing of medical data |
| IN05 | The system shall prevent the unauthorized writing of device identifiers |
| IN06 | The system shall prevent the unauthorized writing of application correlation rules |
| IN07 | The system shall prevent the unauthorized writing of application statistical models |
| IN09 | The system shall prevent the unauthorized writing of application roles |
| IN10 | The system shall prevent the unauthorized writing of application permissions |
| IN11 | The system shall prevent the unauthorized writing of application events |
| IN12 | The system shall prevent the unauthorized writing of application details |
| IN13 | The system shall prevent the unauthorized writing of the IoT identity |
| IN14 | If a system operator asks to register a user without an associated identifier, then the system shall decline the request |
| IN15 | If a system operator asks to register a user with an identifier that it is already in use, then the system shall decline the request |
| IN16 | If a network operator asks to configure the network slices for a non-existing application, then the system shall decline the request |
| IN17 | If a security operator asks to configure the logging mechanism without indicating an application, then the system shall decline the request |
| IN18 | If a security operator asks to configure the logging mechanism for a non-existing application, the system shall decline the request |
| IN19 | If a security operator asks to configure the access control without indicating an application, then the system shall decline the request |
| IN20 | If a security operator asks to configure the access control of a non-existing application, then the system shall decline the request |
| IN21 | If a data operator asks to store some initial medical data without the associated identifiers, then the system shall decline the request |

| | |
|------|---|
| IN22 | If a data operator asks to store some initial medical data with an identifier that is already in use, then the system shall decline the request |
| IN23 | If a data operator asks to store some initial medical data for a non-existing application, then the system shall decline the request |
| IN24 | If a network operator asks to register a mobile device without specifying the device identifier, the system shall decline the request |
| IN25 | If an application asks to store some medical data without the associated identifiers, then the system shall decline the request |
| IN26 | If an application asks to store some medical data with an identifier that is already in use, then the system shall decline the request |
| IN27 | If an application asks to assign an IoT device without specifying the user identifier, then the system shall decline the request |
| IN28 | the system shall reject any request that includes input parameters that the system cannot validate |

IV.3. Non-repudiation

We denote by *Non-repudiation* the degree to which actions or events can be proven to have taken place, so that occurred events or actions cannot be repudiated later [21]. The non-repudiation requirements of ProTego are as in Table 34.

Table 34. Non-repudiation requirements

| Identifier | Requirement |
|------------|--|
| NR01 | When there is an attempt to register a new user, the system shall log the occurrence as an event |
| NR02 | When there is an attempt to conduct the first-time assessment of the infrastructure, the system shall log the occurrence as an event |
| NR03 | When there is an attempt to assess prospective risks to the infrastructure, the system shall log the occurrence as an event |
| NR04 | When there is an attempt to install an application, the system shall log the occurrence as an event |
| NR05 | When there is an attempt to configure the network slices of an application, the system shall log the occurrence as an event |
| NR06 | When there is an attempt to configure the logging mechanism of an application, the system shall log the occurrence an event |
| NR07 | When there is an attempt to specify the access control of an application, the system shall log the occurrence as an event |
| NR08 | When there is an attempt to register the initial medical data of an application, the system shall log the occurrence as an event |
| NR09 | When there is an attempt to register a mobile device, the system shall log the occurrence as an event |
| NR10 | When there is an attempt to store some medical data, the system shall log it as an application event |
| NR11 | When there is an attempt to retrieve some medical data, the system shall log it as an application event |
| NR12 | When there is an attempt to assign an IoT device to an application user, the system shall log the occurrence as an event |
| NR13 | When there is an unsuccessful attempt to log a custom application event, the system shall log it as an application event |
| NR14 | When a mobile agent reports a suspicious activity, the system shall record the activity |
| NR15 | When a security operator asks to review new risks evaluation, the system shall log it as an event |

IV.4. Confidentiality

Confidentiality indicates the degree to which the system ensures that data are accessible only to those authorized to have access [21]. We report in Table 35 the confidentiality requirements of ProTego.

Table 35. Confidentiality requirements

| Identifier | Requirement |
|------------|---|
| CF01 | The system shall prevent the unauthorized reading of infrastructure models |
| CF02 | The system shall prevent the unauthorized reading of events |
| CF03 | The system shall prevent the unauthorized reading of user identities |
| CF04 | The system shall prevent the unauthorized reading of medical data |
| CF05 | The system shall prevent the unauthorized reading of device identifiers |
| CF06 | The system shall prevent the unauthorized reading of application correlation rules |
| CF07 | The system shall prevent the unauthorized reading of application statistical models |
| CF08 | The system shall prevent the unauthorized reading of application roles |
| CF09 | The system shall prevent the unauthorized reading of application permissions |
| CF10 | The system shall prevent the unauthorized writing of application events |
| CF11 | The system shall prevent the unauthorized reading of application details |
| CF12 | The system shall prevent the unauthorized reading of IoT identity |

IV.5. Availability

We define *Availability* as the degree to which a system is operational and accessible when required for use [21]. Table 36 reports the availability requirements of ProTego.

Table 36. Availability requirements

| Identifier | Requirement |
|------------|---|
| AV01 | The system shall prevent one or more users from successfully flooding it with legitimate requests |
| AV02 | The system shall prevent one or more application users from successfully flooding an application with legitimate requests |
| AV03 | The system shall prevent one or more applications from successfully flooding it with legitimate custom application events |

IV.6. Authorization

Authorization is concerned with restrictions on the actions of authenticated users [22]. The authorization requirements of ProTego are illustrated in Table 37.

Table 37. Authorization requirements

| Identifier | Requirement |
|------------|--|
| AZ01 | The system shall only allow system operator to register new users |
| AZ02 | The system shall only allow security operators to conduct first-time risk assessment |
| AZ03 | The system shall only allow security operators to assess prospective risks to the infrastructure |
| AZ04 | The system shall only allow system operators to install applications |
| AZ05 | The system shall only allow network operators to configure the network slices of an application |
| AZ06 | The system shall only allow security operators to configure the logging mechanism of an application |
| AZ07 | The system shall only allow security operators to specify the access control of an application |
| AZ08 | The system shall only allow system operators to store the initial medical data of an application |
| AZ09 | The system shall only allow network operators to register mobile devices |
| AZ10 | The system shall only allow security operators to configure the continuous authentication agent on the mobile device |
| AZ11 | The system shall only allow security operators to respond to alerts |
| AZ12 | The system shall only allow security operators to review alerts |

| | |
|------|--|
| AZ13 | While an application permission allows it, when an application user requests some medical data, the system shall process the request |
| AZ14 | While no application permission allows it, if an application user requests some medical data, then the system shall decline the request |
| AZ15 | While an application permission allows it, when an application user requests to store some medical data, the system shall process the request |
| AZ16 | While no application permission allows it, if an application user requests to store some medical data, then the system shall decline the request |
| AZ17 | When an application user requests to be assigned to an IoT device, the system shall process the request |
| AZ18 | When an authenticated application requests to log a custom application event, the system shall process the request |
| AZ19 | If an unauthenticated application requests to log a custom application event, then the system shall decline the request |
| AZ20 | When an IoT device requests to send medical data securely, while the IoT device is assigned to application user, then the system shall process the request |

IV.7. Detectability

Detectability is defined as the degree to which a system detects, and records attempted access or modification by unauthorized individuals [24]. Detectability is especially important in relation to other quality attributes. For instance, integrity mechanisms only work to the extent that integrity failures generate alerts that are addressed by a person [26]. The detectability requirements of ProTego are shown in Table 38.

Table 38. Detectability requirements

| Identifier | Requirement |
|------------|--|
| DT01 | The system shall alert of any unauthorized attempt to write an infrastructure model |
| DT02 | The system shall alert of any unauthorized attempt to write an event |
| DT03 | The system shall alert of any unauthorized attempt to write a user identity |
| DT04 | The system shall alert of any unauthorized attempt to write medical data |
| DT05 | The system shall alert of any unauthorized attempt to write device identifiers |
| DT06 | The system shall alert of any unauthorized attempt to write application correlation rules |
| DT07 | The system shall alert of any unauthorized attempt to write application statistical models |
| DT08 | The system shall alert of any unauthorized attempt to write application roles |
| DT09 | The system shall alert of any unauthorized attempt to write application permissions |
| DT10 | The system shall alert of any unauthorized attempt to write application details |
| DT11 | The system shall alert of any unauthorized attempt to write IoT identity |
| DT12 | The system shall alert of any unauthorized attempt to read infrastructure models |
| DT13 | The system shall alert of any unauthorized attempt to read events |
| DT14 | The system shall alert of any unauthorized attempt to read user identities |

| | |
|------|---|
| DT15 | The system shall alert of any unauthorized attempt to read medical data |
| DT16 | The system shall alert of any unauthorized attempt to read device identifiers |
| DT17 | The system shall alert of any unauthorized attempt to read application correlation rules |
| DT18 | The system shall alert of any unauthorized attempt to read application statistical models |
| DT19 | The system shall alert of any unauthorized attempt to read application roles |
| DT20 | The system shall alert of any unauthorized attempt to read application permissions |
| DT21 | The system shall alert of any unauthorized attempt to read application details |
| DT22 | The system shall alert of any unauthorized attempt to read IoT identity |

IV.8. Data protection

Data protection pertains to the processing of personal data wholly or partly by automated means. In particular, the processing should be tailored in a way that respects the key data protection principles, as dictated by [25].

Table 39. Data protection requirements

| Identifier | Requirement |
|------------|--|
| DP01 | The system shall guarantee its users their right to erasure |
| DP02 | The system shall apply storage limitation to the personal data processed in the system |
| DP03 | The system shall guarantee its users their right to portability |
| DP04 | The system shall guarantee its users their right to restriction of processing |
| DP05 | The system shall guarantee its users the access to personal data in a timely manner in the event of a physical or technical incident |

V. Nutritional Case Study

In this section, we present the Nutritional case study for the ProTego project, which – together with the Electronic Health Record case study of Section VI, constitute the demonstration applications for the project. More specifically, we start by providing a general overview of *FoodCoach*, a food recommendation system that will act as the *Application*, as per the roles of Section III.2. Then, we present the stakeholders of FoodCoach in the same vein as what has already been presented for ProTego itself. We proceed by introducing the personas for FoodCoach, and the related user roles. After that, we report the main scenario of interaction with the FoodCoach platform and its generalization as a set of use cases.

V.1. Overview

FoodCoach is a food recommendation system that suggests *Personalized Nutrition Plans* (PNPs) to end-users, who access the platform via a responsive Web application (Figure 5). The purpose of the platform is to guide patients towards healthy behaviors. It does so by acting as a mediator between nutritionists and patients. Via the platform, patients consult their personalized food suggestions that have been prepared beforehand by their nutritionist. Patients are recommended to input information into the platform by compiling a food diary so as to attest their adherence to the nutritionist's prescription. Such data can in turn be leveraged by nutritionists to adjust the suggestions as the patient progresses towards his goal (e.g., weight loss).

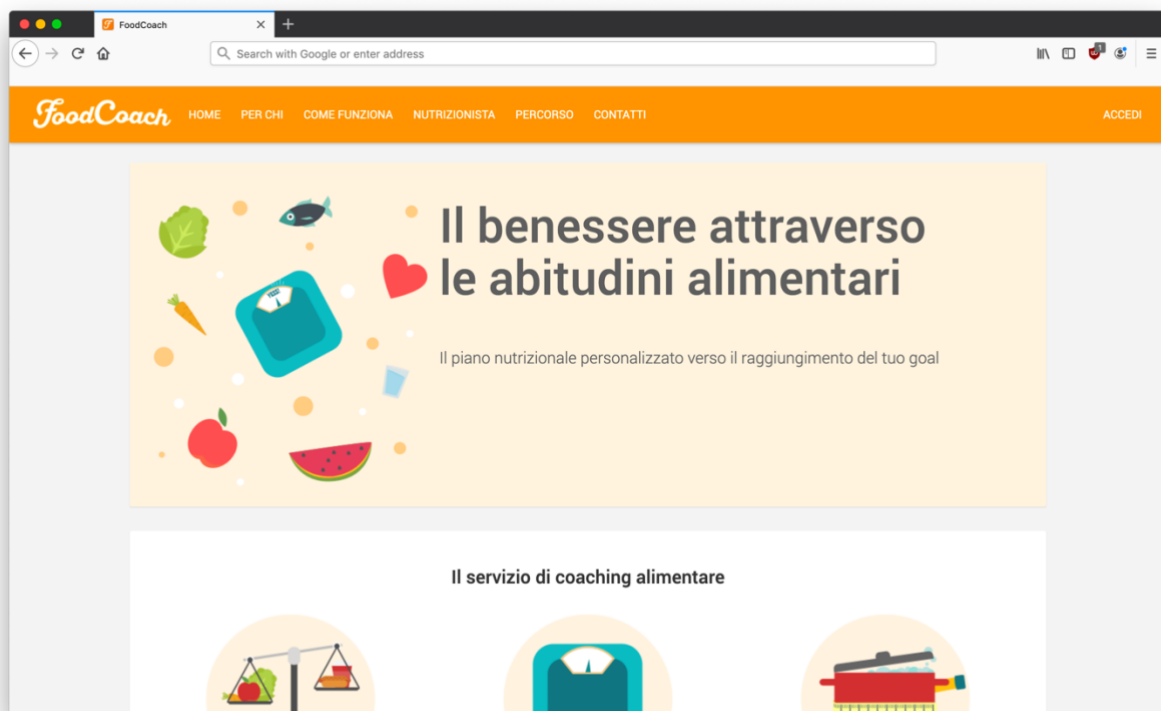


Figure 5. FoodCoach homepage

As far as back-office functionalities are concerned, FoodCoach supports nutritionists in their activities thanks to its ability of automatically compiling nutrition plans and generating aggregated reports.

V.2. Stakeholders

In the case of the FoodCoach platform, too, it is useful to represent its stakeholders by means of a stakeholder map, which we report in Figure 6.

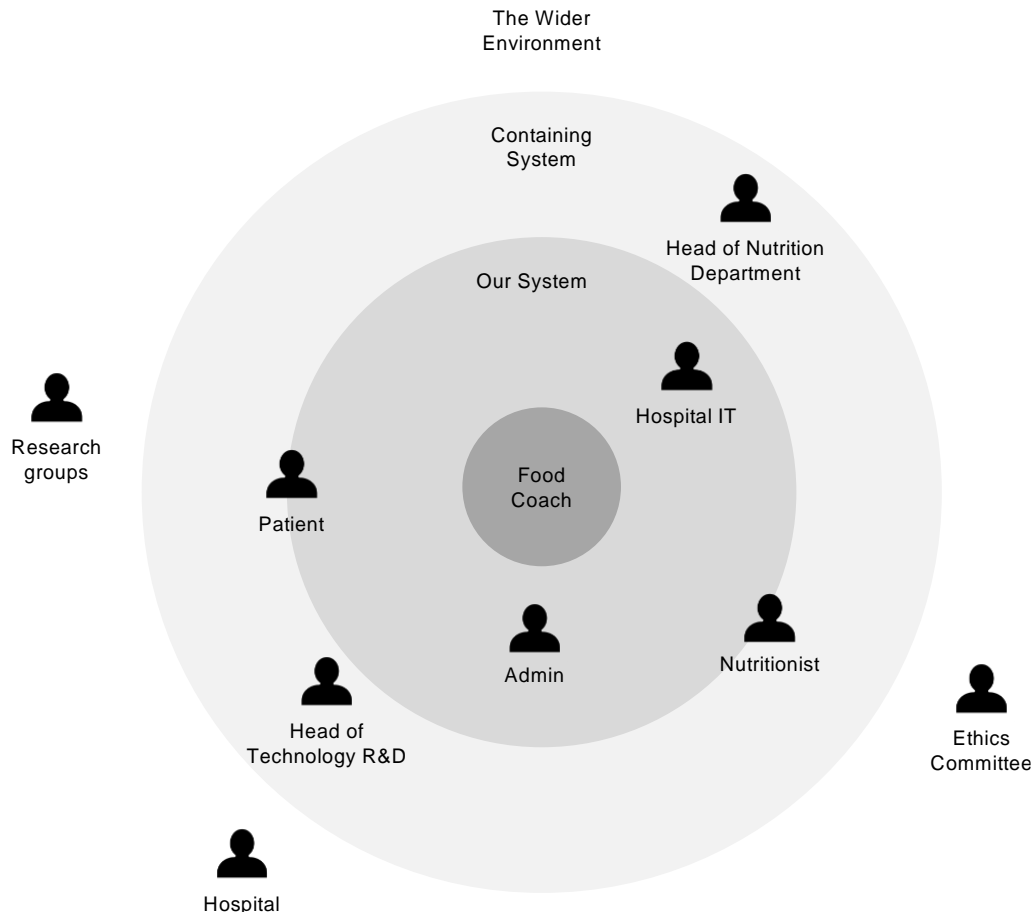


Figure 6. Stakeholder map of the FoodCoach platform

As shown, a distinctive feature of FoodCoach is that *normal operators*, i.e., users that operate the system to deliver value to functional beneficiary, are functional beneficiary themselves. In other words, patients and nutritionists interact with FoodCoach for their own benefit. We show this by placing them at the boundary of the innermost ring. In addition to them, we recognize the Hospital IT as the *maintenance operators*, in that they are responsible for keeping the system up and running within the hospital infrastructure. Finally, we also include the FoodCoach administrator, who acts as a superuser of the platform.

The remaining functional beneficiaries of FoodCoach are the Head of the Technology R&D of the hospital, who commissioned the development of the service – being therefore both the owner and the sponsor – as well as the Head of Nutrition Department.

The wider environment includes indirect stakeholders, namely, research groups, which may later make use of the nutrition data collected for research purposes, the ethics committee, which supervise the appropriateness of the hospital offer from an ethics standpoint, and the hospital at large.

V.3. Personas

Our investigation on the class of users of FoodCoach leads to the development of three primary personas: Elisa – the nutritionist, Antonella – the patient, and Manuel – the application admin. Their profiles are reported in Table 40-Table 42, respectively.

Table 40. Elisa, the “nutritionist” persona


| | |
|--|--|
|  <p><i>“I take care of patients’ health from both a physiological and mental perspective”</i></p> | |
| User role | Nutritionist |
| Description | Elisa, 28 years old. She has been a nutritionist for 4 years. She is responsible for creating PNPs for patients that need to change their nutritional habits in order to either lose, gain, or maintain weight. Though she does not treat diseases, the plans she develops take into account pre-existing conditions and the prevention of disease onset. |
| Goals | Her goal is to create PNPs that improve patients’ health from both a physiological and mental perspective. Towards this end, she checks their measurements (such as height, weight, circumference), calculate their Body Mass Index (BMI), and provide interpretations. Moreover, she tracks nutritional habits, updating their PNP when necessary. |
| Needs & opportunity | <ul style="list-style-type: none"> • She visits patients face to face, and she uses the phone/email to book appointments, answers question and provides support between examinations • She does not use software to create a meal plan. She uses a computer to take notes, store patients’ records, and track their progress • When discussing with patients, she writes notes on paper and handwrites on the Food Diary or other printouts (e.g., anamnesis) • She asks patients to write in the Food Diary what they eat and how they feel, which might be related to what they are eating |

Table 41. Antonella, the “patient” persona



| | |
|---|---|
|  <p><i>“I want to improve my lifestyle in an easy and enjoyable way”</i></p> | |
| User role | Patient |
| Description | Antonella, 27 years old, works as an engineer for a consulting firm. She is a positive person. She likes to feel good and stay in shape. Health is very important to her and she feels like she has it under control, though from time to time she falls into temptation. When this happens, she tries to make up for it during the following days. She can be very disciplined, but she is so busy at work that sometimes her routine gets disrupted. This affects her mood, especially when she does not have time to exercise every day. |
| Goals | She would like to move to a healthy and regular lifestyle in a fairly easy and enjoyable way. She believes that it is important to eat healthy and on time, and to have good physical and mental health. |
| Needs & opportunity | <ul style="list-style-type: none"> • She needs recommendations that fit her lifestyle and a plan to help her stay on target • She needs time-saving tips • She needs a guide to what to eat and how to cook it • She needs a reminder on when to eat and hydrate • She would like to do some physical activities |

Table 42. Manuel, the “admin” persona

| | |
|---|---|
|  <p><i>“I ensure the rest of the staff with an adequate support to work efficiently”</i></p> | |
| User role | Admin |
| Description | <p>Manuel, 46 years old. He works as an admin in the nutritional department of the hospital.</p> <p>He is responsible for managing the adoption and maintenance of software and hardware facilities for the department. In particular, he communicates both with the IT department and the vendors in order to adopt, install, update, tune and diagnose the applications.</p> <p>On his typical day, he deals with a set of activities, among which: analyzing applications problems and report it, setting service accounts, publishing maintenance schedule.</p> |
| Goals | His goal is to maintain the applications up and running in order to guarantee an adequate support to the rest of the staff |
| Needs & opportunity | <ul style="list-style-type: none"> • He needs approvals and support from IT department to integrate requested equipment |

V.4. Storyboard

The storyboard of the Nutritional Scenario is depicted in Table 43. In particular, we mainly focus on the course of interactions going on between Elisa, the nutritionist, and Antonella, her new patient. Throughout the course of events, we show how FoodCoach helps them accomplishing their own particular goals.

Table 43. Storyboard between the patient and the nutritionist, as mediated by FoodCoach

Step 1

Manuel is notified that FoodCoach has been installed in the hospital infrastructure



Step 2

Manuel setups the accounts for the nutritionist via FoodCoach



Step 3

Antonella goes to the hospital for her nutrition examination



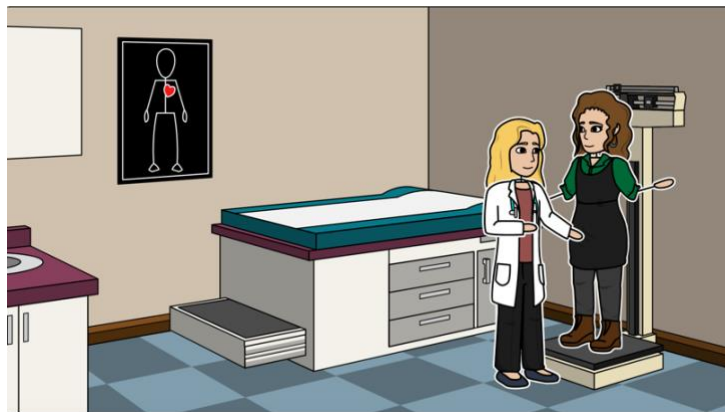
Step 4

Elisa registers Antonella on the platform



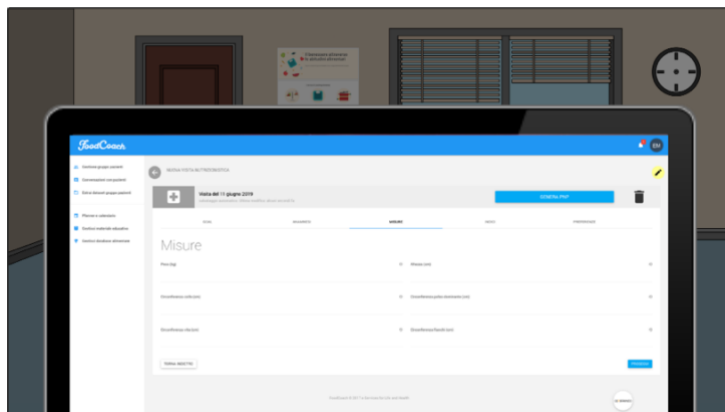
Step 5

Elisa examines Antonella and collects her diet goal, anamnesis, measures, index, preferences, etc.



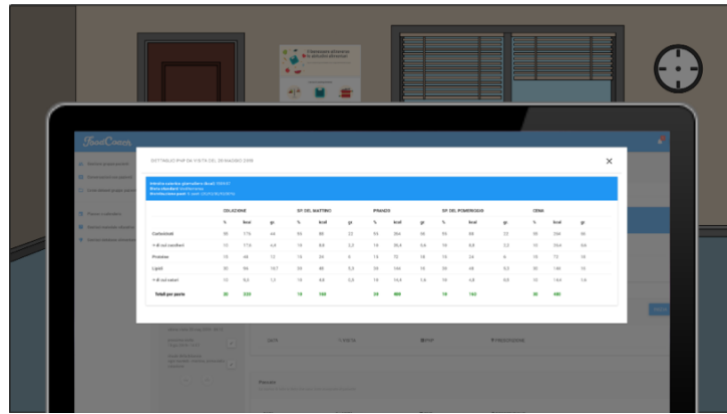
Step 6

Elisa inputs Antonella's data into the platform



Step 7

Elisa prepares Antonella's PNP by specifying her calories intake, the diet type and the distribution of meals



Step 8

Elisa completes Antonella's examination by asking her food preferences



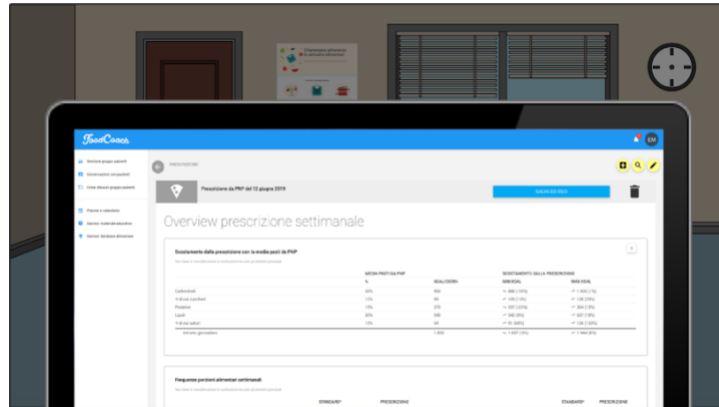
Step 9

Elisa provides Antonella with the device to monitor physical activity before dismissing her



Step 10

From the PNP, and by setting the food consumption, Elisa publishes Antonella's prescription



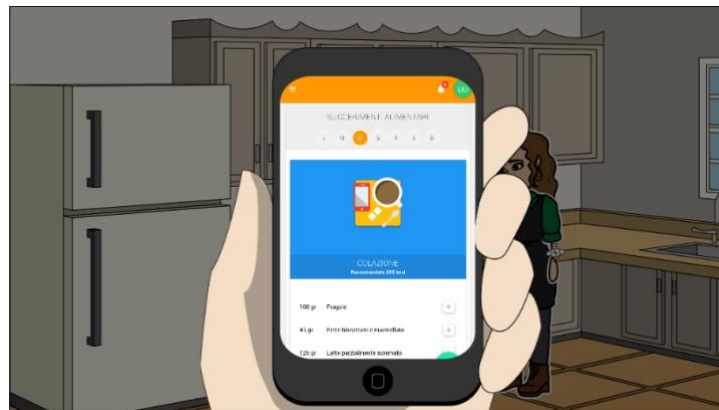
Step 11

Antonella starts her diet and, when it is time to cook, she accesses FoodCoach



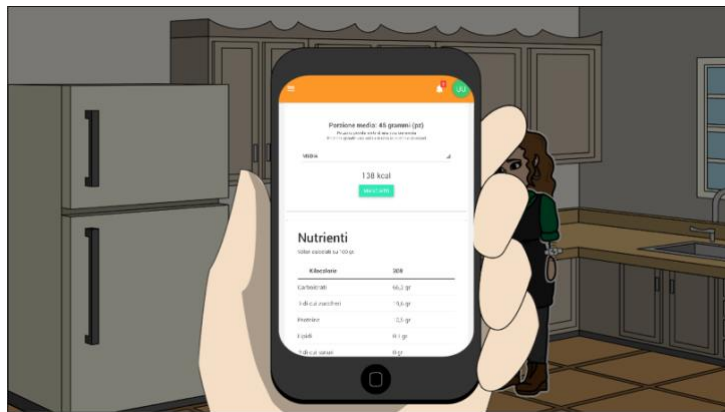
Step 12

Antonella consults the "Food suggestion" section, where she finds the suggested meal for the different times of the day



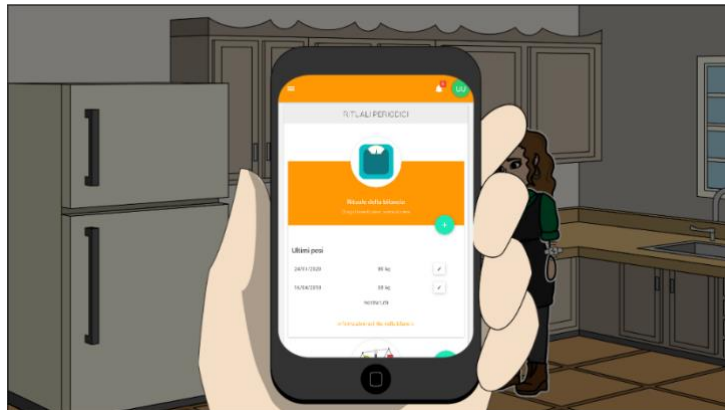
Step 13

Antonella compiles the "Foods Diary" by entering the foods she consumed during the day



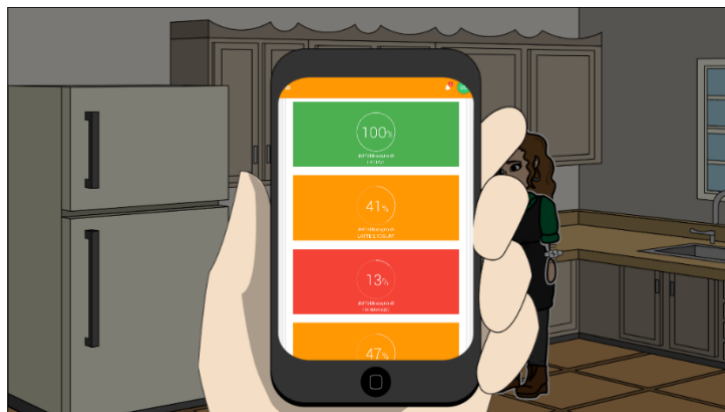
Step 14

Once a week, Antonella registers her weight in the platform to keep track of her progress



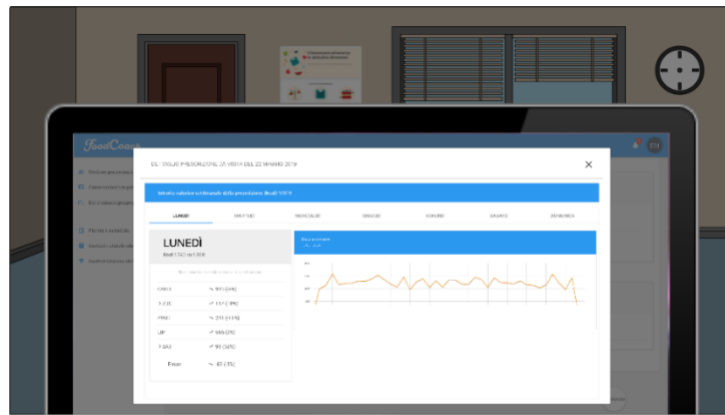
Step 15

Antonella accesses the statistics page of the platform to consult aggregated reports



Step 16

In the meantime, Elisa queries the platform for aggregated statistics



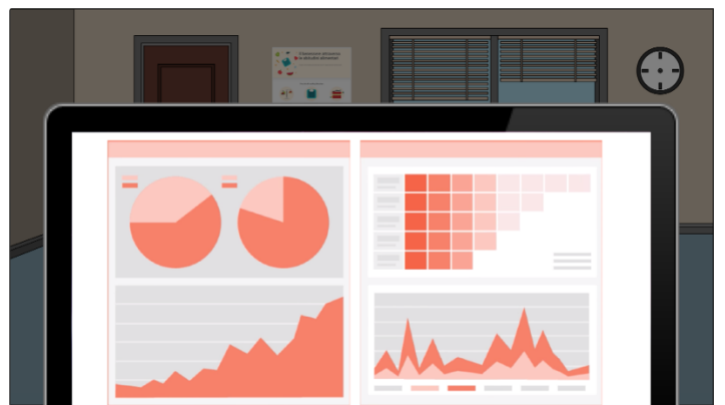
Step 17

Antonella goes back to the hospital to check her progress. Elisa downloads Antonella's physical activity data from her device



Step 18

Elisa accesses to relevant statistics about Antonella's physical activity



V.5. Roles

FoodCoach includes three different user roles. Specifically, we considered patients and nutritionists, together with administrations, who carry out supervisory tasks. They are reported in detail in Table 44.

Table 44. User roles of the FoodCoach platform

| User role | Description |
|--------------|--|
| Patient | Patients interact with the platform in order to obtain nutrition suggestions and to keep track of their progress and habits |
| Nutritionist | Nutritionists take care of preparing patients' suggestions in response to patients' calories intake, weight, and BMI changes. They also record parameters of interest collected as part of face-to-face examinations |
| Admin | Administrators carry out supervisory tasks, such as registering nutritionists to the platform |

V.6. Use Cases

The core use cases of FoodCoach are summarized in Figure 7. As shown, the use case diagram is partitioned into two disjoint sets of use cases; namely, a set of back-office use cases to support the nutritionist and the administrator, and a set of front-office uses cases related to the patient. Detailed descriptions of all use cases are reported from Table 45 to Table 56.

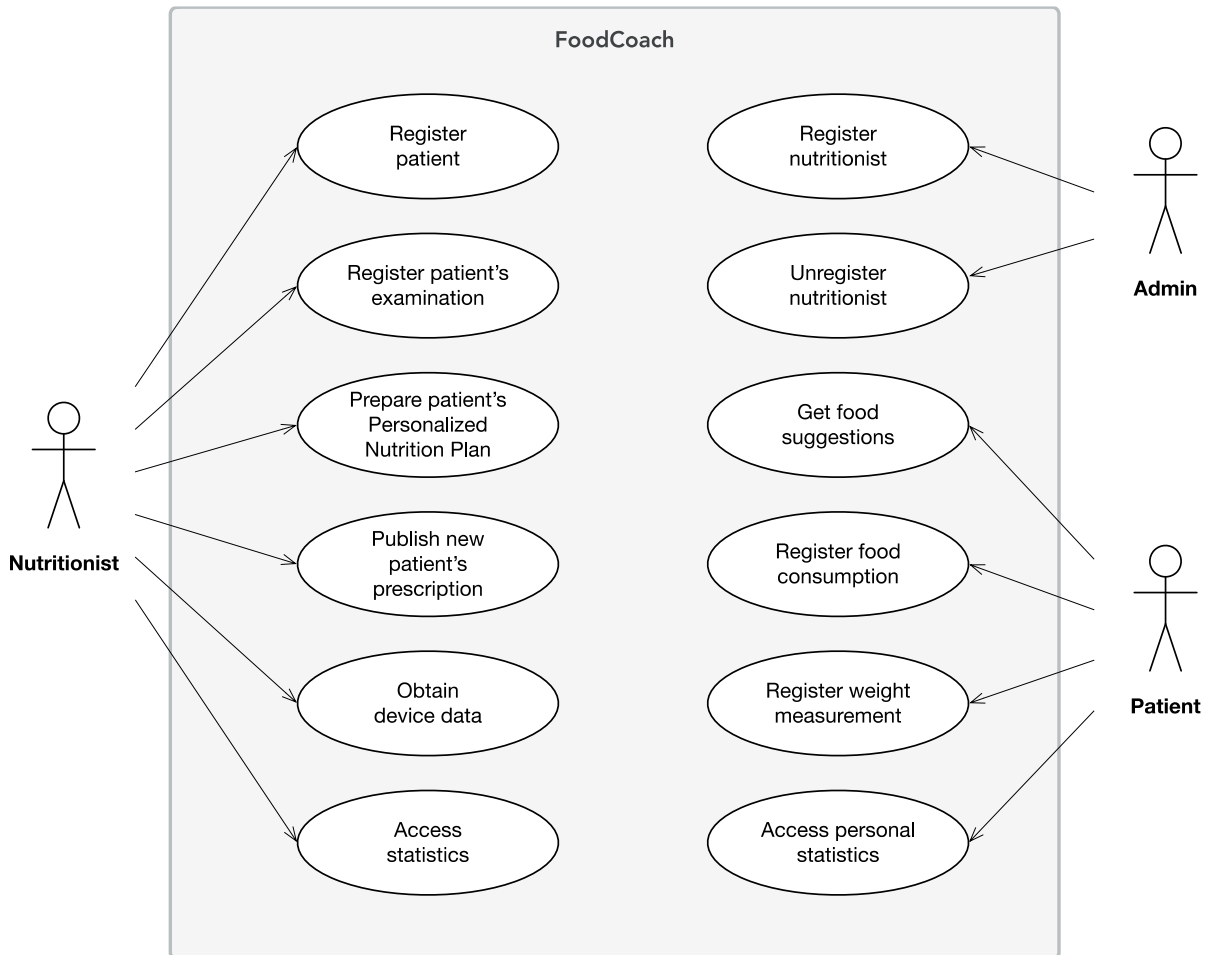


Figure 7. Use case diagram of the FoodCoach platform

Table 45. “Register nutritionist” use case

| | |
|----------------------|--|
| Identifier | OSR-UC01 |
| Goal | Register nutritionist |
| Actor | Admin |
| Trigger | A new nutritionist is assigned to the management of patients |
| Precondition | 1. Admin has logged into the system |
| Success guarantee | 1. Nutritionist is registered on the system 2. System sends to the nutritionist an e-mail with a link to access the platform |
| Success scenario | 1. Admin provides the registration details (e.g., name and surname) 2. System registers the nutritionist |
| Exceptional scenario | E1. Nutritionist is already registered 1. System reports error: “Nutritionist already registered” 2. System terminates the use case |

Table 46. “Unregister nutritionist” use case

| | |
|-------------------|--|
| Identifier | OSR-UC02 |
| Goal | Unregister nutritionist |
| Actor | Admin |
| Trigger | Nutritionist leaves the nutritionist department |
| Precondition | 1. Admin has logged into the system |
| Success guarantee | 1. Nutritionist is unregistered from the system 2. System sends to the physician an e-mail informing that the access is no longer possible for the nutritionist |
| Success scenario | 1. Admin selects the nutritionist under consideration 2. Admin asks to unregister the nutritionist 3. System unregisters the nutritionist |

Table 47. “Register patient” use case

| | |
|----------------------|---|
| Identifier | OSR-UC03 |
| Goal | Register patient |
| Actor | Nutritionist |
| Trigger | Nutritionist takes care of a new patient |
| Precondition | 2. Nutritionist has logged into the system |
| Success guarantee | 3. Nutritionist’s patient is registered on the system 4. System sends to the patient an e-mail with credentials to access the platform |
| Success scenario | 3. Nutritionist provides the registration details (e.g., name and surname) 4. System registers the patient |
| Exceptional scenario | E1. Patient is already registered 3. System reports error: “Patient already registered” 4. System terminates the use case |

Table 48. “Register patient’s examination” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC04 |
| Goal | Register patient’s examination |
| Actor | Nutritionist |
| Trigger | Nutritionist examines the patient in person |
| Precondition | <ol style="list-style-type: none"> 1. Nutritionist has logged into the system 2. Nutritionist’s patient is still to be examined for the first time |
| Success guarantee | <ol style="list-style-type: none"> 1. Patient’s examination is registered in the system |
| Success scenario | <ol style="list-style-type: none"> 1. Nutritionist selects the record of the patient of interest 2. Nutritionist asks to create a new examination 3. Nutritionist enters the examination report 4. System registers the patient’s examination |

Table 49. “Prepare patient’s Personalized Nutrition Plan” use case

| | |
|--------------------------|--|
| Identifier | OSR-UC05 |
| Goal | Prepare patient’s Personalized Nutrition Plan |
| Actor | Nutritionist |
| Trigger | Patient needs a revised Personalized Nutrition Plan |
| Precondition | <ol style="list-style-type: none"> 1. Nutritionist has logged into the system 2. Examination of the nutritionist’s patient is present in the system |
| Success guarantee | <ol style="list-style-type: none"> 1. Patient’s PNP is generated and stored |
| Success scenario | <ol style="list-style-type: none"> 1. Nutritionist selects the record of the patient of interest 2. Nutritionist asks to automatically compute the PNP 3. Nutritionist provides required parameters (e.g., daily calories intake) 4. System calculates the PNP 5. Nutritionist accepts the generated PNP (7) or asks for personalizing the plan (6) 6. Nutritionist manually personalizes the PNP, by changing the composition of calories and nutrients 7. System stores the PNP |

Table 50. “Publish new patient’s prescription” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC06 |
| Goal | Publish new patient’s prescription |
| Actor | Nutritionist |
| Trigger | Nutritionist needs to publish a new prescription for a patient of hers |
| Precondition | <ol style="list-style-type: none"> 1. Nutritionist has logged into the system 2. PNP of nutritionist’s patient is present in the system |
| Success guarantee | <ol style="list-style-type: none"> 1. A new prescription is published to the patient |
| Success scenario | <ol style="list-style-type: none"> 1. Nutritionist selects the record of the patient of interest 2. Nutritionist asks to automatically generate a new prescription from a PNP of choice 3. System calculates a new prescription 4. Nutritionist accepts the prescription (6) or asks to personalize it (5) 5. Nutritionist manually personalizes the prescription, by changing the selection of foods 6. System stores and publishes the prescription |

Table 51. “Access statistics” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC07 |
| Goal | Access statistics |
| Actor | Nutritionist |
| Trigger | Nutritionist needs to access to application statistics |
| Precondition | <ol style="list-style-type: none"> 1. Nutritionist has logged into the system |
| Success guarantee | <ol style="list-style-type: none"> 1. Nutritionist is made aware of statistics |
| Success scenario | <ol style="list-style-type: none"> 1. Nutritionist asks to access statistics of a patient of interest 2. The system returns statistics of his patients (e.g., average weight progression over time) |

Table 52. “Obtain device data” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC08 |
| Goal | Obtain device data |
| Actor | Nutritionist |
| Trigger | Nutritionist is visiting the patient as part of a follow up examination |
| Precondition | <ol style="list-style-type: none"> 1. Nutritionist has logged into the system |
| Success guarantee | <ol style="list-style-type: none"> 1. Nutritionist obtains device data |
| Success scenario | <ol style="list-style-type: none"> 1. Nutritionist plugs the device to her computer 2. Nutritionist asks to download data from the device 3. The system downloads data from device |

Table 53. “Get food suggestions” use case

| | |
|--------------------------|--|
| Identifier | OSR-UC09 |
| Goal | Get food suggestions |
| Actor | Patient |
| Trigger | Patient wants to see what to eat in the next few days |
| Precondition | <ol style="list-style-type: none"> 1. Patient has logged into the system 2. Patient’s nutritionist published his prescription |
| Success guarantee | <ol style="list-style-type: none"> 1. Patient is informed on what to eat next |
| Success scenario | <ol style="list-style-type: none"> 1. Patient asks to access the suggested foods 2. System returns the suggested foods for each meals of the day 3. If needed, patient accesses details about foods nutrients 4. If needed, patient assesses the food alternatives |

Table 54. “Register food consumption” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC10 |
| Goal | Register food consumption |
| Actor | Patient |
| Trigger | Patient needs to register food consumption |
| Precondition | <ol style="list-style-type: none"> 1. Patient has logged into the system |
| Success guarantee | <ol style="list-style-type: none"> 1. Patient has registered the food consumed |
| Success scenario | <ol style="list-style-type: none"> 1. Patients asks to register food consumption 2. Patients enters food consumption entries 3. System saves information |

Table 55. “Register weight measurement” use case

| | |
|--------------------------|---|
| Identifier | OSR-UC11 |
| Goal | Register weight measurement |
| Actor | Patient |
| Trigger | Patient is reminded via a notification to register his weight |
| Precondition | <ol style="list-style-type: none"> 1. Patient has logged into the system |
| Success guarantee | <ol style="list-style-type: none"> 1. Patient’s weight has been registered |
| Success scenario | <ol style="list-style-type: none"> 1. Patient asks to register a new weight measurement 2. Patient enters his weight measurement 3. System saves the information |

Table 56. "Access personal statistics" use case

| | |
|--------------------------|--|
| Identifier | OSR-UC12 |
| Goal | Access personal statistics |
| Actor | Patient |
| Trigger | Patient needs to access personal statistics |
| Precondition | 1. Patient has logged into the system |
| Success guarantee | 1. Patient is made aware of his statistics |
| Success scenario | 1. Patient asks to access personal statistics 2. The system returns patient statistics (e.g., his weight progression over time) |

VI. Electronic Health Record Case Study

This section is devoted to the presentation of the Electronic Health Record (EHR) Case Study of the ProTego toolkit. To this end, we introduce Pocket EHR, a platform that allows both patients and physicians to access relevant data stored as part of the hospital EHRs. We then illustrate its stakeholders by way of a stakeholder map. We continue by analyzing the user personas of Pocket EHR, and the corresponding user roles. After presenting a storyboard depicting the main course of interactions between the patient and the physician, we conclude the discussion on Pocket EHR by detailing its core use cases.

VI.1. Overview

Pocket EHR is a platform that allows both patients and physicians to access relevant data stored as part of the hospital electronic health records. By means of Pocket EHR, patients can check if their upcoming appointments have been scheduled, and later review the results of their diagnostic tests. In addition, Pocket EHR provides a direct communication channel between patients and their physician, permitting patients to feedback relevant information even without the need of face-to-face meetings.

Pocket EHR enables mobile access to electronic health records, providing a convenient and unified access point capable of abstracting the underlying Health Information System (HIS). As a result, it is possible to provide an easy-to-use consultation service to patients and doctors alike, while at the same time adopting a unified EHR, which allows the hospital to implement holistic patient care processes.

In order to ensure minimal exposure of the hospital infrastructure, the parts of the EHR of interest to the Pocket EHR will be available from outside of the on-premises system. In this regard, ProTego makes possible the utilization of external resources and infrastructure while assuring a trusted data exchange.

VI.2. Stakeholders

The stakeholder map of Pocket EHR is depicted in Figure 8. As shown, the direct stakeholders are physicians, who consult the health data of a patient while mobile, likely because they are out of the hospital premises; and patients, who are interested in accessing their health test results and use the platform to send health-related communications to their physicians. As with FoodCoach, such classes of users are both normal operator and functional beneficiaries of the platform, for they use the platform for their own benefit. The maintenance operators include the IT provider, which is responsible for ensuring the system is up and running, and the Pocket EHR administrator, who takes care of supervisory tasks in the platform.

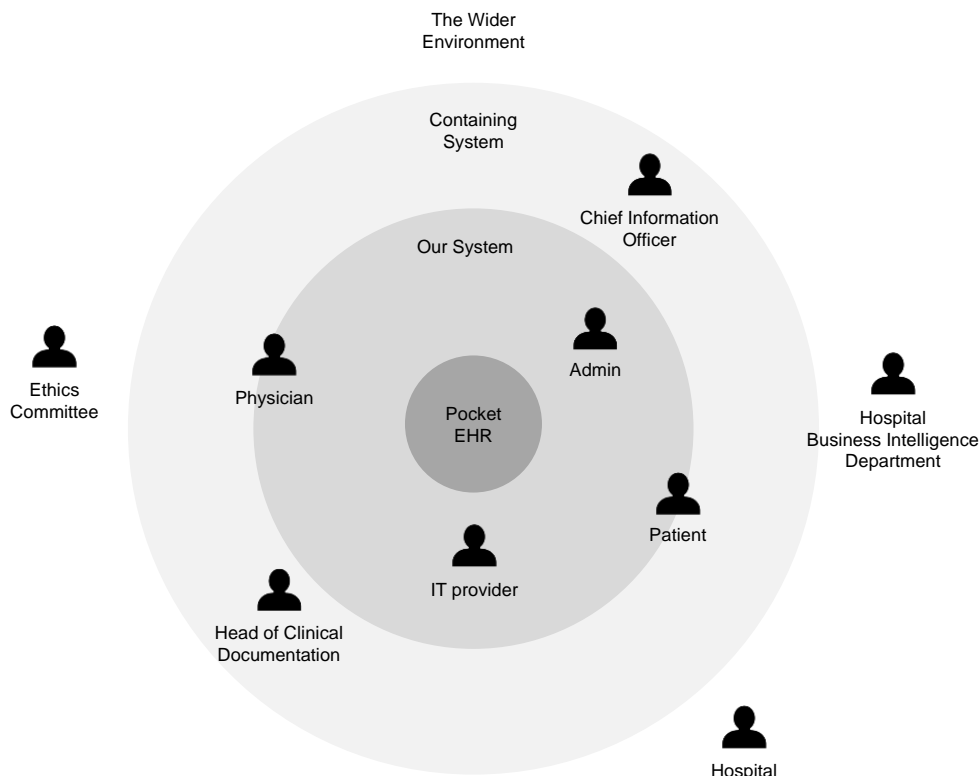


Figure 8. Stakeholder map of Pocket EHR

Other functional beneficiaries are the Head of Clinical Documentation, who supervises the information to be published, and the Chief Information Officer, who is the technical promoter and responsible of the project.

As far as indirect stakeholders are concerned, the Hospital Business Intelligence department and the Ethics Committee are responsible of monitoring how much the system is used and the impact of the system in terms of benefits. Finally, the system is predictably of interest to the hospital itself.

VI.3. Personas

We identified three primary user personas that distill who might be interested in interacting with Pocket EHR, namely, Julio – the physician, Javier – the patient, and Iago – the application admin. Their profiles are reported in Table 57-Table 59, respectively.

Table 57. Julio, the “physician” persona


| | |
|--|---|
|  <p><i>“I need to constantly monitor the progress of my patients, taking early actions to avoid acute episodes”</i></p> | |
| User role | Physician |
| Description | Julio, 32 years old, has been a cardiologist for four years. He takes care of patients with diagnosed with chronic heart failure. He inspects patient’s periodic diagnostic tests and reacts as needed, asking the patient to schedule a visit, order a new test, and so on. |
| Goals | <p>His goal is to control the progress of their patients, taking early actions to avoid acute episodes for their patients.</p> <p>To achieve this, he orders periodic blood tests, ECGs, Holter and stress tests, depending on the patient status. Furthermore, he needs patient status feedback as input to determine appropriate further actions.</p> <p>Patients feel safe because they know their health status is being monitored and the doctor is taking care of them even if no face-to-face visits occur.</p> |
| Needs & opportunity | <ul style="list-style-type: none"> • He wants to empower and train patients as much as possible, making patients an active and responsible part of their healthcare • He wants to avoid patient visits face to face when not necessary, which is common with this type of patient. In fact, as these patients are trained and empowered, many of the result notifications and communications can be made without physical presence • He needs a channel for asynchronously communicating relevant information to patients • He wants to receive from patients updates about their status (how they feel), which are important factors to take decisions |

Table 58. Javier, the “patient” persona



| | |
|---|--|
|  <p><i>“I steadily report my health condition to physicians so that I rapidly act in case of need”</i></p> | |
| User role | Patient |
| Description | <p>Javier, 56 years old, is a schoolteacher.</p> <p>He has been suffering from a chronic health failure since 2016, so he understands he needs periodic controls to check that his health problem is under control. Since then, he has become familiar with the clinical test names, and the normalcy ranges for him, so when he has periodic visits with his physicians to discuss results, he can already tell if the results are ok.</p> <p>He is a disciplined person and takes his health problem seriously and accomplishes all the instructions his doctor gives.</p> <p>He lives about 50 km far from the hospital so visiting the hospital implies a 100 km travel.</p> |
| Goals | He is completely involved in his healthcare and knows that he can avoid problems by following up the indications he receives from doctors. |
| Needs & opportunity | <ul style="list-style-type: none"> • He needs to have updated information about his status • He needs a way to report his doctor how he feels • He needs to minimize required visits to the hospital |

Table 59. Iago, the “admin” persona

| | |
|---|--|
|  <p><i>“I ensure the rest of the staff with an adequate support to work efficiently”</i></p> | |
| User role | Admin |
| Description | <p>Iago, 32 years old. He works as a member of the IT department of the hospital.</p> <p>He is responsible of performing maintenance tasks for in-house applications in the Hospital, including deployments, role management and issues management.</p> <p>On his typical day, he deals with a set of activities, among which: analyzing applications problems and report it, setting service accounts, publishing maintenance schedule.</p> |
| Goals | His goal is maintaining the applications up and running to guarantee the rest of the staff with an adequate support to work efficiently. |
| Needs & opportunity | He needs utilities that let him control issues, misbehaviours and threats as quick and efficient as possible |

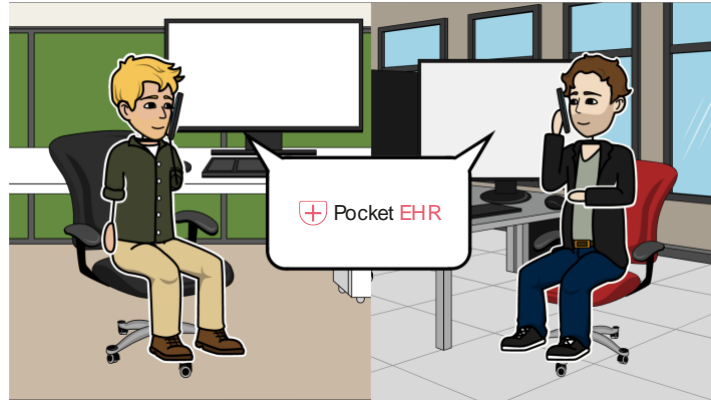
VI.4. Storyboard

The storyboard of the Electronic Health Record case study is reported in Table 60. It depicts the main course of interactions going on between Julio – the physician, and Javier – his patient, and how Pocket EHR supports them in achieving their respective goals.

Table 60. Storyboard between the patient and the physician, as mediated by Pocket EHR

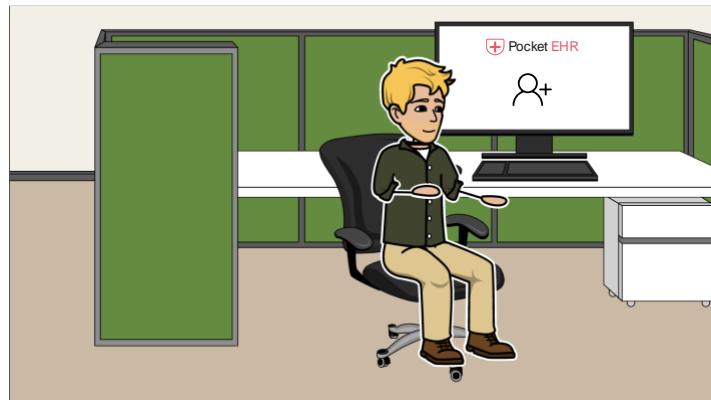
Step 1

Iago is notified that Pocket EHR has been installed in the hospital infrastructure



Step 2

Iago setups the physicians' accounts in Pocket EHR



Step 3

Javier goes to the hospital for his diagnostic test with his doctor Julio



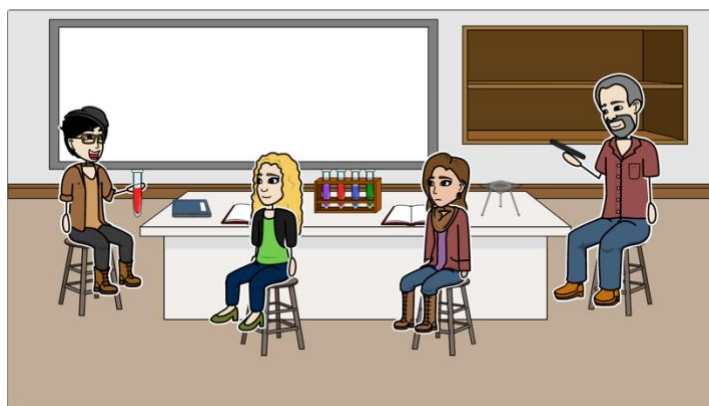
Step 5

Before dismissing him, Julio gives to Javier a device to monitor his physical activity and asks him to install Pocket EHR on his mobile device



Step 6

After a few days, Javier checks the result of his test



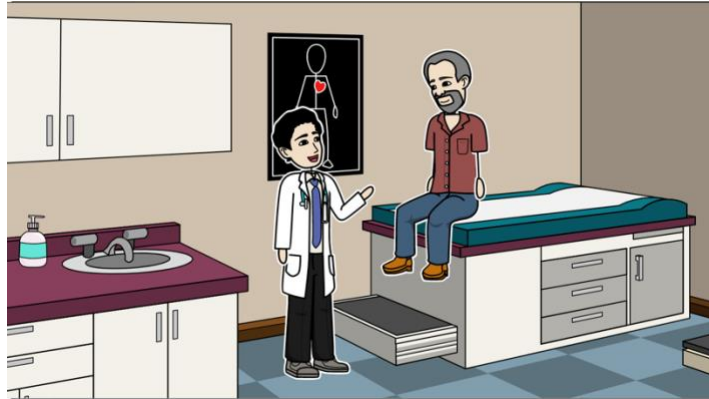
Step 7

Javier checks its upcoming recurrent appointment



Step 8

Javier goes to the hospital for a specialist visit with Julio. On that occasion, Julio asks Javier to use Pocket EHR to periodically report how he feels



Step 9

Javier reports relevant information about his health status



Step 10

Physical activity data are transferred from the device to the smartphone, integrating Javier reports



Step 11

Although out of office, Julio reviews the reports that Javier provided



VI.5. Roles

Pocket EHR involves three different user roles. More precisely, we recognize the roles of physicians, patients and Pocket EHR administrator. Their details are reported in Table 61.

Table 61. User roles of the Pocket EHR platform

| User role | Description |
|-----------|--|
| Patient | Patients interact with the platform in order to check for new appointments and to inspect test results. They also report relevant information to their physician |
| Physician | The physician exploits the platform by gathering patient's information |
| Admin | Administrators carry out supervisory tasks, such as registering physician to the platform |

VI.6. Use Cases

The core use cases of Pocket EHR are depicted in Figure 9. As shown, use cases naturally divide into three groups. Specifically, the first group of use cases comprises front-office functionalities meant for the patients, such as the possibility of checking for new appointments. In addition, we include back-office functionalities for the physicians, such as the possibility to consult, in mobility, data related to his patients. Lastly, we provide the administrator with user management capabilities. Use cases are explained in depth from Table 62 to Table 70.

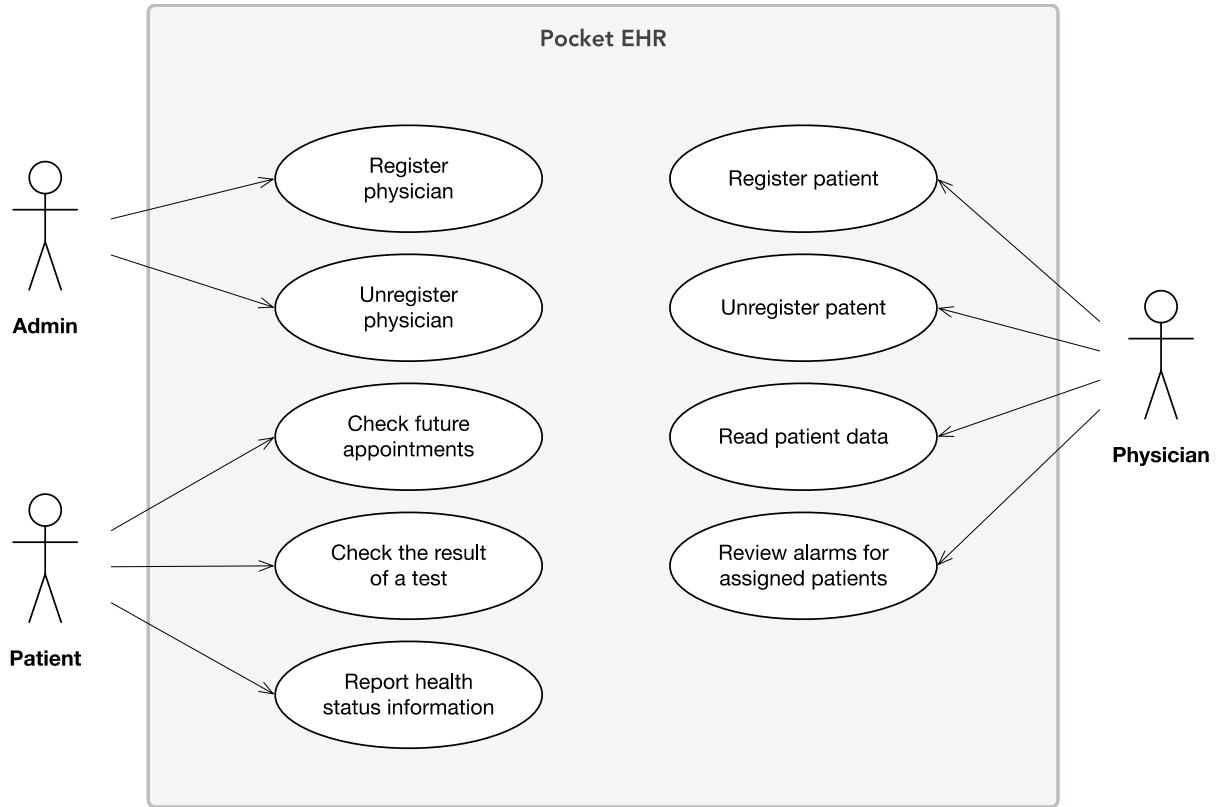


Figure 9. Use case diagram of Pocket EHR

Table 62. “Register physician” use case

| | |
|-----------------------------|--|
| Identifier | Marina-UC01 |
| Goal | Register physician |
| Actor | Admin |
| Trigger | New physician ingress to the remote care program |
| Precondition | 1. Admin has logged into the system |
| Success guarantee | 1. Physician is registered on the system 2. System sends to the physician an e-mail with a link to access the platform |
| Success scenario | 1. Admin provides the physician’s registration details (name, surname, care program, etc.) 2. System registers the physician |
| Exceptional scenario | E1. Physician is already registered 2. System reports error: “Physician already registered” 3. System terminates the use case |

Table 63. “Unregister physician” use case

| | |
|--------------------------|--|
| Identifier | Marina-UC02 |
| Goal | Unregister physician |
| Actor | Admin |
| Trigger | A physician leaves the remote care program |
| Precondition | 1. Admin has logged into the system |
| Success guarantee | 1. Physician is unregistered from the system 2. System sends to the physician an e-mail informing that the access is no longer possible for the physician |
| Success scenario | 1. Admin select the physician under consideration 2. Admin asks to unregister the physician 3. System unregisters the physician |

Table 64. “Register patient” use case

| | |
|----------------------|---|
| Identifier | Marina-UC03 |
| Goal | Register patient |
| Actor | Physician |
| Trigger | A patient fits the criteria to be included into a remote care program |
| Precondition | 1. Remote patient's registry is accessible from the hospital |
| Success guarantee | 1. Patient is registered on the system 2. System sends to the patient an e-mail with a link to access the platform |
| Success scenario | 1. Physician opens the patient's encounter 2. Physician asks for the inclusion of the patient into the remote care program 3. System include the patient in the remote care program |
| Exceptional scenario | E1. Patient is already registered 3. System reports error: “Patient already registered” 4. System terminates the use case |

Table 65. “Unregister patient” use case

| | |
|----------------------|---|
| Identifier | Marina-UC04 |
| Goal | Unregister patient |
| Actor | Physician |
| Trigger | A patient fits the criteria to leave a remote care program |
| Precondition | 1. Remote patient's registry is accessible from the hospital |
| Success guarantee | 1. Patient is unregistered from the system 2. System sends to the patient an e-mail informing that the access is no longer possible for the user |
| Success scenario | 1. Physician opens the patient's encounter 2. Physician ask for the exclusion of the patient from the remote care program 3. System excludes the patient from the remote care program |
| Exceptional scenario | E1. Patient does not exist 3. System reports error: “Patient does not exist” 4. System terminates the use case |

Table 66. “Read patient's registered data” use case

| | |
|-------------------|---|
| Identifier | Marina-UC05 |
| Goal | Read patient's registered data |
| Actor | Physician |
| Trigger | Physician needs to review patient reported status |
| Precondition | 1. Physician is logged into the system |
| Success guarantee | 1. Physician reads information entered by the patient |
| Success scenario | 1. Physician selects the patient from a list of managed patients 2. Physician asks to access patient's data 3. System displays the patient's data |

Table 67. “Review alarms for assigned patients” use case

| | |
|--------------------------|---|
| Identifier | Marina-UC06 |
| Goal | Review alarms for assigned patients |
| Actor | Physician |
| Trigger | Physician needs to review patients that need to be contacted due to its reported health status |
| Precondition | 1. Physician is logged into the system |
| Success guarantee | 1. Physician accesses the list of managed patients that raised an alarm |
| Success scenario | <ol style="list-style-type: none"> 1. Physician asks for the list of managed patients that raised an alarm 2. System displays the list of managed patients that raised an alarm |

Table 68. “Check for future appointments” use case

| | |
|--------------------------|---|
| Identifier | Marina-UC07 |
| Goal | Check future appointments |
| Actor | Patient |
| Trigger | 1. Patient needs to check future scheduled appointments |
| Precondition | 1. Patient has logged into the system |
| Success guarantee | 1. Patient is informed of his future appointments |
| Success scenario | <ol style="list-style-type: none"> 1. Patient asks to access his agenda 2. System displays patient’s agenda, showing the scheduled appointments, if any |

Table 69. “Check the result of a test” use case

| | |
|--------------------------|---|
| Identifier | Marina-UC08 |
| Goal | Check the result of a test |
| Actor | Patient |
| Trigger | Patient is waiting for some test result to be published |
| Precondition | 1. Patient has logged into the system |
| Success guarantee | 1. Patient is informed of the test result, if any |
| Success scenario | <ol style="list-style-type: none"> 1. Patient selects the test of interest 2. System displays test details 3. If the test result is available, patient asks to view it 4. System displays the test result |

Table 70. "Report health status information" use case

| | |
|--------------------------|--|
| Identifier | Marina-UC09 |
| Goal | Report health status information |
| Actor | Patient |
| Trigger | System asks the patient to report relevant information |
| Precondition | 1. Patient has logged into the system |
| Success guarantee | 2. Relevant information is saved in the system |
| Success scenario | 1. Patient completes the prompted health status report 2. Patient submits the health status report 3. System stores the health status report |

VII. Real-life Situations

In this section, we illustrate a number of real-life situations in which patients' safety, data privacy and infrastructures are put at risk, in the context of a project case study. Situations are summarized in Table 71, and investigated in detail in the next sections.

Table 71. Real-life situations overview

| Real-life situation | Case study | Description |
|----------------------------------|------------|--|
| Stealing a device | FoodCoach | An attacker steals the nutritionist's mobile phone and attempts to access her data. ProTego detects that the attacker does not match nutritionist's behavioral pattern, thus raising an alert from this occurrence |
| Unauthorized request | FoodCoach | ProTego receives a data access request, together with an authorization token, which however does not grant the permission to carry out the required operation. ProTego rejects the request and raises an alert |
| Tampering with medical data | FoodCoach | ProTego is subjected to an unauthorized attempt to access and modify the stored data. ProTego protects the data at rest and raises an alert |
| Sniffing traffic from IoT device | Pocket EHR | An attacker intercepts a data transfer between the patient's IoT device and his smartphone. Upon retransmission, ProTego rejects the data and raises an alert |
| Spoofing IoT device | FoodCoach | An attacker attempts to get possession of the user's identity to illegitimately send some data. ProTego prevent the attacker from stealing the user's identity |

VII.1. Stealing a device

The first real-life situation we present is concerned with an attacker that steals the mobile phone of a FoodCoach nutritionist in the attempt of accessing her data. The detailed storyboard is depicted in Table 72.

Table 72. “Stealing a device” real-life situation

Step 1

Elisa uses FoodCoach in her daily activities to provide assistance to her patient Antonella



Step 2

While Elisa is using FoodCoach



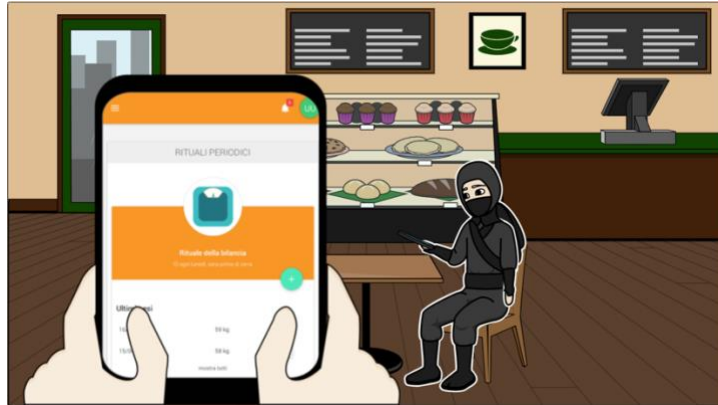
Step 3

An attacker steals her phone



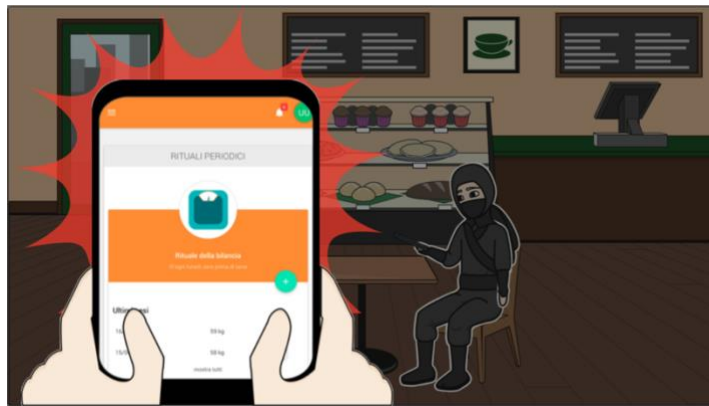
Step 4

The attacker accesses FoodCoach application



Step 5

After a while, the ProTego mobile device security mechanism detects that the attacker does not match Elisa's behavioral pattern



Step 6

At the nth report, the events are interpreted as a possible malicious usage of the device. An alert is therefore sent to Andrew



VII.2. Unauthorized request

In this section, we introduce a second real-life situation involving the improper usage of authorization tokens with the aim of carrying out escalation of privileges in the context of the Nutritional case study. The associated storyboard is reported in Table 73.

Table 73. “Unauthorized request” real-life situation

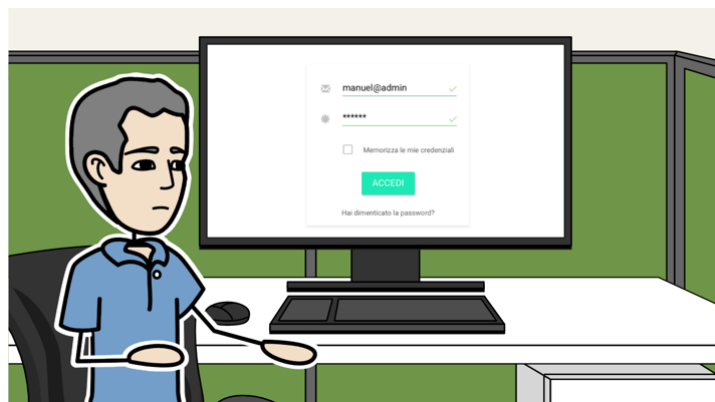
Step 1

Manuel wants to profit from his role as FoodCoach admin by attempting to access Antonella’s data



Step 2

Manuel logs with his own credential in FoodCoach. As a result, FoodCoach receives a valid authorization token for Manuel



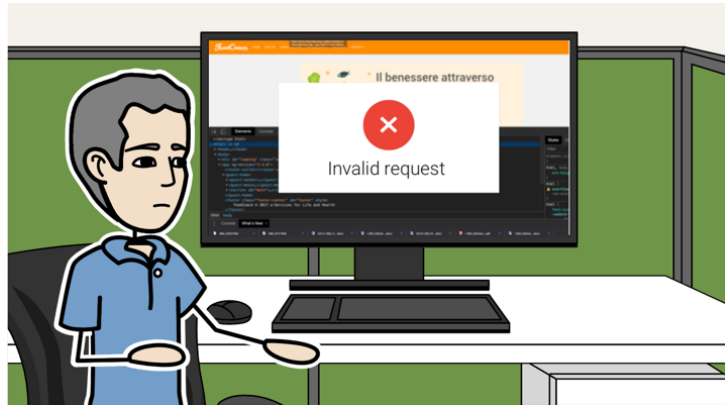
Step 3

Manuel tampers with the FoodCoach application, managing to issue a request containing his token and asking to see Antonella’s weights



Step 4

ProTego rejects his request, since no valid authorization token from Antonella is presented, and logs the unsuccessful attempt to retrieve medical data



Step 5

Andrew receives an alert that a data access operation was rejected due to an invalid authorization token



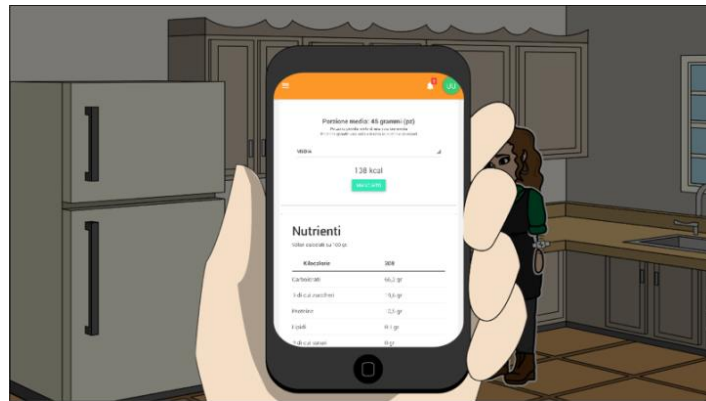
VII.3. Tampering with medical data

In the third real-life situation, ProTego is subjected to an unauthorized attempt to access and modify the medical data of the FoodCoach application. Still, as shown in Table 74, the system is able to protect the data at rest and raise an alert.

Table 74. “Tampering with medical data” real-life situation

Step 1

Antonella uses the FoodCoach on her mobile phone to record the meal portions she consumes



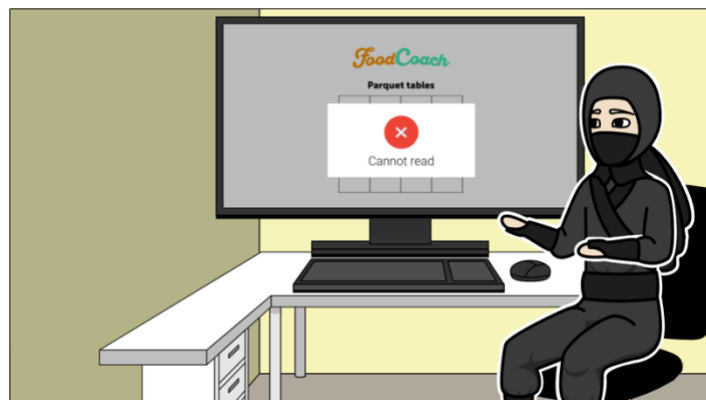
Step 2

An attacker is able to gain access to the file system where the encrypted medical data are stored



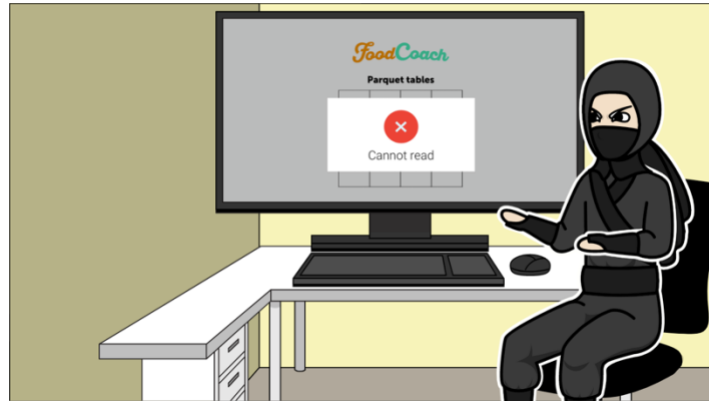
Step 3

The attacker tries reading the medical data but without the encryption keys, no reader can open them



Step 4

The attacker decides therefore to cause a wrong analysis of the data



Step 5

The attacker surreptitiously changes the content of a file. Since the content is encrypted, he randomly changes a number of bytes



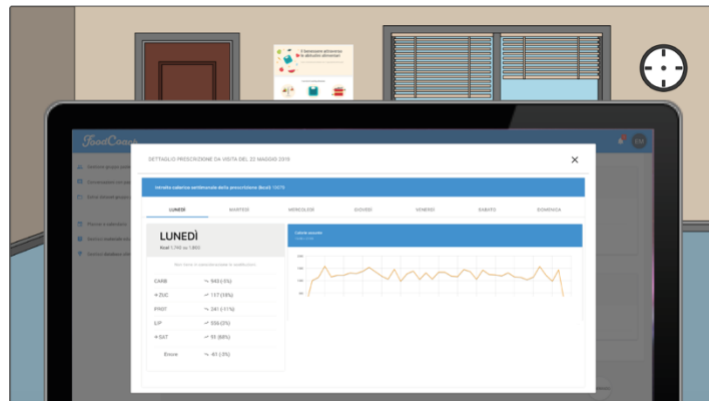
Step 6

In addition, the attacker creates his own medical data in order to skew analysis results and the nutrition recommendations. Since he does not know the encryption keys, he decides to create the medical data without encryption, and to insert his data alongside the legitimate ones



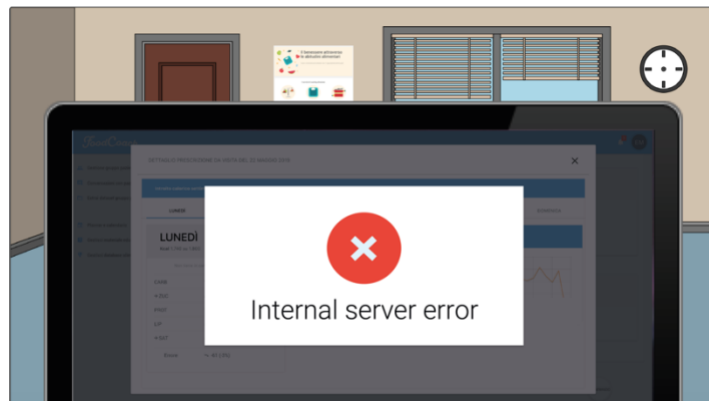
Step 7

Later that day, Elisa decides to review Antonella's progress



Step 8

As soon as ProTego encounters the spurious data, it throws an error



Step 9

Consequently, ProTego communicates to Andrew the improper modification by raising an alert



Step 10

Andrew is quickly able to detect that there was an attempt to tamper with the stored data. He takes steps to secure the data store, and then restores the medical data from backup



VII.4. Sniffing traffic from IoT device

The fourth real-life situation deals with the unauthorized interception of data flowing from a Pocket EHR patient’s device to his smartphone. The related storyboard is depicted in Table 75.

Table 75. “Sniffing traffic from IoT device” real-life situation

Step 1

Javier is taking his time to complete his health status report, while enjoying a coffee in a bar



Step 2

He is doing it unaware of the fact that an attacker is intercepting the wireless data transfer between his device and ProTego



Step 3

The attacker manages to sniff the data, but he cannot read the content, as it is encrypted



Step 4

At that point, the attacker tries to perform a replay attack



Step 5

However, these messages are rejected because the communication is secured from this attack



Step 6

This generates an alert regarding the fact that a network attack may have taken place



VII.5. Spoofing IoT identity

The fifth and last real-life situation describes the case of an attacker trying to spoof the identity of an IoT device. The details are reported in the storyboard of Table 76.

Table 76. “Spoofing IoT device” real-life situation

Step 1

Antonella is hosting a party at her place, unaware of the fact that an attacker is among the invitees



Step 2

Using an excuse, the attacker asks to connect to Antonella's Wi-Fi on his smartphone



Step 3

From his smartphone, the attacker intercepts the Wi-Fi traffic to retrieve the connection parameters, along with the identity credentials



Step 4

The attacker wants to impersonate Antonella's device but the information he retrieved is encrypted so that he cannot access to the identity credentials



VIII. Metrics

In this section, we present the final set of metrics for ProTego, which specify the indicators that stakeholders will use to define and measure success on this project [16]. In particular, we provide evidence on the verification of the functionalities, of the non-functional qualities, as well as on the usability of the proposed solution.

VIII.1. Functional success rate

The first metric we introduce is the *Functional success rate*, that is, the fraction of implemented scenarios over the total amount of scenarios describing the system functionalities and presented from Table 77 to Table 102.

In order to measure the *Functional success rate*, we specify a set of *acceptance tests*, that is, the examples of the requirements in action [27]. In particular, we articulate acceptance tests using the “*Given, When, Then*” pattern, a well-established approach for conveying acceptance tests ([28], [29]). In accordance with the adopted formalism, for each of them we describe alternative scenarios of execution – whether successful or unsuccessful, in terms of the required preconditions (the *Given* part), the event or action causing the interaction (the *When* part), and the expected outcome resulting from such an interaction (the *Then* part)¹. At the same time, the different scenarios also exercise different quality attributes of the system, e.g., its authorization mechanism.

The initial set of metrics is reported from Table 78 to Table 102. Collectively, they exercise the system in 73 distinct test scenarios. For convenience, Figure 10 repeats the personas of both ProTego, FoodCoach and Pocket EHR, who are actors in the acceptance tests.










| IT operators | | Case study users | | | | | Attackers |
|---|---|---|---|---|--|---|---|
|  |  |  |  |  |  |  |  |
| Andrew | Carlo | Manuel | Elisa | Antonella | Javier | Julio | Attacker |
| Data op. Security op. System op. | Network op. | Admin (FoodCoach) | Nutritionist (FoodCoach) | Patient (FoodCoach) | Patient (Pocket EHR) | Physician (Pocket EHR) | - |

Figure 10. ProTego, FoodCoach and Pocket EHR personas, including the attacker

In addition, we also include the attacker from the real-life situations of Section VII. In this regard, we denote scenarios describing real-life situation with the  icon.

¹ For increased readability, successive *Given's*, *When's* or *Then's* are often replaced with *And's* and *But's*

Table 77. Acceptance tests of the “Deploy cluster” use case

Scenario: Operator deploys the cluster

Given Andrew is acting as an System Operator of the infrastructure
And The virtual machines have been prepared for the deployment
And The master node and the worker nodes have been configured
When Andrew asks to deploy the cluster on the machines
Then Andrew should be able to deploy the cluster

Scenario: Insufficient authorization

Given Andrew is not acting as an System Operator of the infrastructure
When Andrew asks to deploy the cluster
Then Andrew should be notified that he cannot deploy the cluster

Table 78. Acceptance tests of the “Install Data Gateway” use case

Scenario: Operator installs Data Gateway

Given Andrew is acting as System Operator
And Andrew installed the FHIR server, the Query Gateway and the Access Control Framework
When Andrew asks to install the Data Gateway
Then The Data Gateway should be installed in the infrastructure

Scenario: Insufficient authorization

Given Andrew is not acting as System Operator
When Andrew asks to install the Data Gateway
Then Andrew should be notified that he cannot install the Data Gateway

Table 79. Acceptance tests of the “Install Network Slicing” use case

Scenario: Operator installs Network Slicing

Given Andrew is acting as System Operator
And Andrew installed the Network Slicing controller and the access point
And Andrew registered the access point in the Network Slicing controller
When Andrew asks to install the Network Slicing
Then The Network Slicing should be installed in the infrastructure

Scenario: Insufficient authorization

Given Andrew is not acting as System Operator
When Andrew asks to install the Network Slicing
Then Andrew should be notified that he cannot install the Network Slicing

Scenario: Access point already registered

Given Andrew is acting as System Operator
And An access point has already been registered with ID abc123
When Andrew asks to register an access point with ID abc123
Then Andrew should be notified that he cannot register the access point

Table 80. Acceptance tests of the “Install SIEM” use case

Scenario: Operator installs SIEM

Given Andrew is acting as System Operator

And Andrew installed the SIEM log analyzer and the SIEM agent

And Andrew configured a mechanism to redirect logs from the application to the SIEM agent

When Andrew asks to install the SIEM

Then The SIEM should be installed in the infrastructure

Scenario: Insufficient authorization

Given Andrew is not acting as System Operator

When Andrew asks to install the SIEM

Then Andrew should be notified that he cannot install the SIEM

Table 81. Acceptance tests of the “Install Continuous Authentication” use case

Scenario: Operator installs Continuous Authentication

Given Andrew is acting as System Operator

And Andrew installed the EDR component and the JBCA component

When Andrew asks to install the Continuous Authentication

Then The Continuous Authentication should be installed in the infrastructure

Scenario: Insufficient authorization

Given Andrew is not acting as System Operator

When Andrew asks to install the Continuous Authentication

Then Andrew should be notified that he cannot install the Continuous Authentication

Table 82. Acceptance tests of the “Install SSM” use case

Scenario: Operator installs SSM

Given Andrew is acting as System Operator

When Andrew asks to install the SSM

Then The SSM should be installed in the infrastructure

Scenario: Insufficient authorization

Given Andrew is not acting as root

When Andrew asks to install the SSM

Then Andrew should be notified that he cannot install the SSM

Table 83. Acceptance tests of the “Register user” use case

Scenario: Administrator registers a new user

Given Andrew is acting as an System Operator for a component of the ProTego toolkit
And Andrew has specified the name and associated role of the new operator
When Andrew asks to register the new operator for that component
Then Andrew should be able to register a new operator

Scenario: Insufficient authorization

Given Andrew is not acting as an System Operator for a component of the ProTego toolkit
When Andrew asks to register the new operator for that component
Then Andrew should be notified that he cannot register a new operator

Scenario: User identifier already taken

Given Andrew is acting as an System Operator for a component of the ProTego toolkit
And A new operator has already been registered as operator for that component
When Andrew asks to register the same operator for that component
Then Andrew should be notified that the user already exists

Table 84. Acceptance tests of the “Conduct first-time risk assessment” use case

Scenario: Security operator assesses risks

Given Andrew is a Security operator in ProTego
When Andrew provides the infrastructure model of the hospital to be evaluated
Then Andrew should be made aware of the risks and mitigations actions
And ProTego should store the hospital infrastructure model and the associated risks

Scenario: Insufficient authorization

Given Carlo is not a Security operator in ProTego
When Carlo provides the infrastructure model of the hospital to be evaluated
Then Carlo should be notified that he cannot assess the hospital infrastructure

Scenario: First-time assessment already conducted

Given The infrastructure model is already stored into ProTego
And Andrew is a Security operator in ProTego
When Andrew provides the same infrastructure model to be evaluated
Then Andrew should be notified that the infrastructure model is already stored

Table 85. Acceptance tests of the “Assess prospective risks to the infrastructure” use case

Scenario: Security operator assesses application risks

Given The infrastructure is modeled into ProTego
And Andrew is a Security operator in ProTego
When Andrew provides an infrastructure model that includes a new application
Then Andrew should be made aware of the risks that the new application poses to the infrastructure

Scenario: Insufficient authorization

Given Carlo is not a Security operator in ProTego
When Carlo provides an infrastructure model that includes FoodCoach
Then Carlo should be notified that he cannot assess the risks of applications

Scenario: Prospective risk assessment already conducted

Given The infrastructure model is already stored into ProTego

And Andrew is a Security operator in ProTego
When Andrew provides the same infrastructure model to be evaluated
Then Andrew should be notified that the infrastructure model is already stored

Table 86. Acceptance tests of the “Install application” use case

Scenario: System operator installs a new application

Given Andrew is a System operator in ProTego
When Andrew asks to install FoodCoach
Then Andrew should be able to install FoodCoach

Scenario: Insufficient authorization

Given Carlo is not a System operator in ProTego
When Carlo asks to install FoodCoach
Then Carlo should be notified that he cannot install the application

Scenario: Already existing application

Given FoodCoach has been installed in ProTego
And Andrew is a System operator in ProTego
When Andrew asks to install FoodCoach
Then Andrew should be notified that the application already exists

Table 87. Acceptance tests of the “Configure application network slices” use case

Scenario: Security operator configures network slices

Given FoodCoach has been installed in ProTego
And Carlo is a Network operator in ProTego
When Carlo indicates the network slices, their quality-of-service and the traffic configuration
Then Carlo should be able to configure the network slices

Scenario: Insufficient authorization

Given FoodCoach has been installed in ProTego
And Andrew is not a Network operator in ProTego
When Andrew indicates the network slices configuration of FoodCoach
Then Andrew should be notified he cannot configure application network slices

Scenario: Network slices are already configured

Given FoodCoach has been installed in ProTego
And FoodCoach network slices have been already configured
And Carlo is a Network operator in ProTego
When Carlo indicates the network slices configuration of FoodCoach
Then Carlo should be notified that network slices are already configured

Table 88. Acceptance tests of the “Configure application logging mechanism” use case

Scenario: Security operator specifies logging mechanism

Given FoodCoach has been installed in ProTego
And Andrew is a Security operator in ProTego
When Andrew configures the logging mechanism for FoodCoach
Then Andrew should be able to configure the logging mechanism for FoodCoach

Scenario: Insufficient authorization

Given FoodCoach has been installed in ProTego
And Carlo is not a Security operator in ProTego
When Carlo configures the logging mechanism for FoodCoach
Then Carlo should be notified that he cannot configure the logging mechanism of an application

Table 89. Acceptance tests of the “Specify application access control” use case

Scenario: Security operator specifies access control

Given FoodCoach has been installed in ProTego
And Andrew is a Security operator in ProTego
When Andrew specifies the application access control of FoodCoach
Then Andrew should be able to activate the specified access control

Scenario: Insufficient authorization

Given FoodCoach has been installed in ProTego
And Carlo is not a Security operator in ProTego
When Carlo specifies the application access control of FoodCoach
Then Carlo should be notified that he cannot specify the access control of an application

Table 90. Acceptance tests of the “Configure mobile device” use case

Scenario: Security operator configure continuous authentication agent

Given Continuous authentication component has been installed in ProTego
And Application has been installed in ProTego
When Andrew asks to configure the continuous authentication agent
And Andrew specifies the necessary agent configuration
Then Andrew should be able to activate the specified agent

Scenario: Mobile device already configured

Given Continuous authentication agent has already been configured in the mobile device
When Andrew specifies the necessary agent configuration
Then Andrew should be notified that the agent has already been configured

Table 91. Acceptance tests of the “Store initial medical data” use case

Scenario: Data operator stores initial medical data

Given FoodCoach has been installed in ProTego

And Andrew is a Data operator in ProTego

When Andrew asks to store the initial medical data for FoodCoach

Then Andrew should be able to store the initial medical data for FoodCoach

Scenario: Insufficient authorization

Given FoodCoach has been installed in ProTego

And Carlo is not a Data operator in ProTego

When Carlo asks to store the initial resources for FoodCoach

Then Carlo should be notified that he cannot store the FoodCoach initial medical data

Scenario: Application initial resources are already stored

Given FoodCoach has been installed in ProTego

And FoodCoach initial medical data are stored in ProTego

And Andrew is a Data operator in ProTego

When Andrew asks to store the initial medical data for FoodCoach

Then Andrew should be notified that FoodCoach already features some initial medical data

Table 92. Acceptance tests of the “Register mobile device” use case

Scenario: Network operator registers a new mobile device

Given FoodCoach has been installed in ProTego

And Carlo is a Network operator in ProTego

When Carlo specifies the device identifier

And asks to register Elisa's mobile device

Then Carlo should be able to register Elisa's mobile device

Scenario: Insufficient authorization

Given FoodCoach has been installed in ProTego

And Andrew is not a Network operator in ProTego

When Andrew asks to register Elisa's mobile device

Then Andrew should be notified that he cannot register mobile devices

Scenario: Mobile device is already registered

Given FoodCoach has been installed in ProTego

And Elisa's mobile device has already been registered

And Carlo is a Network operator in ProTego

When Carlo asks to register Elisa's mobile device

Then Carlo should be notified that the device is already registered

Table 93. Acceptance tests of the “Store medical data” use case

Scenario: Nutritionist stores the patient’s medical data

Given FoodCoach is installed in ProTego

And FoodCoach has obtained a valid authorization token for Elisa

When FoodCoach asks to store a medical data associated with Antonella

Then FoodCoach should be able to store the medical data

Scenario Outline: Insufficient authorization

Given FoodCoach is installed in ProTego

And FoodCoach has obtained a valid authorization token for <user>

When FoodCoach asks to store medical data associated with <medical_data_user>

Then FoodCoach should be notified that <user> cannot store medical data of <medical_data_user>

Examples: Insufficient authorization

| | |
|-----------|-------------------|
| user | medical_data_user |
| Admin | Patient |
| Patient01 | Patient02 |
| Patient | Nutritionist |

Scenario: Authorization token is expired

Given FoodCoach is installed in ProTego

And FoodCoach has obtained an expired authorization token for Elisa

When FoodCoach asks to store medical data associated with Antonella

Then FoodCoach should be notified that the authorization token expired

Scenario: Authorization token is ill-formed

Given FoodCoach is installed in ProTego

And FoodCoach has obtained an ill-formed authorization token for Elisa

When FoodCoach asks to store medical data associated with Antonella

Then FoodCoach should be notified that the authorization token is ill-formed

Table 94. Acceptance tests of the “Retrieve medical data” use case

Scenario Outline: Nutritionist queries for some patient's weights

Given FoodCoach is installed in ProTego
And The following medical data were recorded by Elisa in ProTego

| patient | medical_data |
|-----------|--------------|
| Antonella | visit1 |
| Giovanna | visit2 |
| Giovanna | visit3 |

And FoodCoach has obtained a valid authorization token for <nutritionist>
When FoodCoach submits the query to see the medical data of <patient>
Then FoodCoach should receive the result set <medical_data>

Examples: A nutritionist can query for a patient's medical data, but she will only see those for which she's the associated nutritionist

| nutritionist | patient | medical_data |
|--------------|-----------|------------------|
| Elisa | Antonella | [visit1] |
| Elisa | Giovanna | [visit2, visit3] |
| Martina | Antonella | [] |
| Martina | Giovanna | [] |

Scenario: Insufficient authorization

Given FoodCoach is installed in ProTego
And FoodCoach has obtained a valid authorization token for Manuel
When FoodCoach submits the query to see the medical data of Antonella
Then FoodCoach should be notified that Manuel cannot perform such a query

Scenario: Medical data have been tampered with

Given FoodCoach is installed in ProTego
And an attacker was able to tamper with the data containing Antonella’s medical data
And FoodCoach has obtained a valid authorization token for Elisa
When FoodCoach submits the query to see the medical data of Antonella
Then FoodCoach should be notified that the data have been corrupted

Scenario: Authorization token is expired

Given FoodCoach is installed in ProTego
And FoodCoach has obtained an expired authorization token for Elisa
When FoodCoach submits the query to see the medical data of Antonella
Then FoodCoach should be notified that the authorization token expired

Scenario: Authorization token is ill-formed

Given FoodCoach is installed in ProTego
And FoodCoach has obtained an ill-formed authorization token for Elisa
When FoodCoach submits the query to see the medical data of Antonella
Then FoodCoach should be notified that the authorization token is ill-formed

Table 95. Acceptance tests of the “Assign IoT device to application user” use case

Scenario: Patient is assigned a new IoT device

Given Pocket EHR is installed in ProTego
And Javier is one of Julio's patients
And Javier has received an unassigned device
And Pocket EHR has obtained a valid authorization token for Javier
When Pocket EHR asks to assign the device to Javier
Then Pocket EHR should be able to assign the device to Javier

Scenario: Assign IoT device to a new user

Given Pocket EHR is installed in ProTego
And Javier is one of Julio's patients
And Pocket EHR has obtained a valid authorization token for Javier
And The IoT device has already stored an authorization token for another user
When Pocket EHR asks to assign an already assigned device to Javier
Then The IoT device should overwrite the authorization token

Scenario: Insufficient authorization

Given Pocket EHR is installed in ProTego
And Pocket EHR has obtained a valid authorization token for the admin
When Pocket EHR asks to assign an unassigned device to Javier
Then Pocket EHR should be notified that the admin is not authorized to assign devices

Scenario: Authorization token is expired

Given Pocket EHR is installed in ProTego
And Pocket EHR has obtained an ill-formed authorization token for Javier
When Pocket EHR asks to assign an unassigned device to Javier
Then Pocket EHR should be notified that the authorization token expired

Scenario: Authorization token is ill-formed

Given Pocket EHR is installed in ProTego
And Pocket EHR has obtained an ill-formed authorization token for Javier
When Pocket EHR asks to assign an unassigned device to Javier
Then Pocket EHR should be notified that the authorization token is ill-formed

Table 96. Acceptance tests of the “Log custom application event” use case

Scenario: Correct application key

- Given** The agent is installed in ProTego
- And** The analyzer component is installed in ProTego
- When** The agent logs a custom application event by using a key
- Then** The agent should be able to log the custom application event

Scenario: Wrong application key

- Given** FoodCoach is installed in ProTego
- When** FoodCoach sends an erroneous application key and asks to log a custom application event
- Then** FoodCoach should be notified that the application is not authorized

Table 97. Acceptance tests of the “Send medical data securely” use case

Scenario: IoT device sends some medical data securely

- Given** the device has been assigned to Javier
- And** the device has received a valid ID_token for Javier
- When** the device asks to send some medical data
- Then** the medical data should be stored in ProTego

Scenario: Authorization token is ill-formed

- Given** the device has been assigned to Javier
- And** the device has received an ill-formed ID_token for Javier
- When** the device asks to send some medical data
- Then** the device should be notified that the ID_token is ill-formed

Scenario: Expired ID_token

- Given** the device has been assigned to Javier
- And** the device has received an ID_token for Javier
- And** the ID_token for Javier expired
- When** the device asks to send some medical data
- Then** the device should be notified that the ID_token is expired
- And** the device should request a new ID_token using the Refresh_token

Scenario: Protecting against Replay attack 🛡️

- Given** A device has been assigned to Javier
- And** the device is connected to ProTego
- And** the device sent some medical data to ProTego
- And** an attacker intercepted the traffic
- When** the attacker sends again the same medical data
- Then** the attacker transmission should be rejected

Scenario: Protecting against spoofing 🛡️

- Given** A device has been assigned to Javier
- And** the device is connected to ProTego
- And** the device sent some medical data to ProTego
- And** an attacker intercepted the traffic
- When** the attacker tries to read the identity credentials
- Then** the attacker should not be able to read such information because the traffic is encrypted

Table 98. Acceptance tests of the “Report suspicious activity” use case

Scenario: Mobile agent reports suspicious activity 

- Given** Elisa's smartphone is registered in ProTego
 - And** an attacker stole Elisa's phone while in the subway
 - And** the attacker has been using Elisa's phone
 - When** the mobile agent noticed that the attacker does not match Elisa's behavioral pattern
 - Then** the mobile agent should be able report the suspicious activity to ProTego
-

Table 99. Acceptance tests of the “Respond to alert” use case

Scenario: Security operator responds to an alert 

- Given** Manuel attempted to access Antonella's medical data
- And** an alert originated from this unauthorized attempt
- And** Andrew is a Security operator in ProTego
- When** Andrew asks to display the details of the alert
- Then** Andrew should be able to see that Manuel tried to access Antonella's medical data

Scenario: Insufficient authorization

- Given** an alert originated from an unauthorized attempt of accessing data
 - And** Carlo is not a Security operator in ProTego
 - When** Carlo asks to display the details of the alert
 - Then** Carlo should be notified that he cannot see alerts
-

Table 100. Acceptance tests of the “Review alerts” use case

Scenario: Security operator review alerts

- Given** Andrew is a Security operator in ProTego
- When** Andrew asks to review the alerts
- Then** Andrew should be prompted with the alerts

Scenario: Insufficient authorization

- Given** Carlo is not a Security operator in ProTego
 - When** Carlo asks to review the alerts
 - Then** Carlo should be notified that he cannot review alerts
-

Table 101. Acceptance tests of the “Review new risk evaluation” use case

Scenario: Security operator reviews changes in the evaluation

Given The infrastructure and its risks are modeled into ProTego

And Andrew is a Security operator in ProTego

When Andrew checks if there are changes in the risk assessment

Then Andrew should be prompted with the new evaluation, if any

Scenario: Insufficient authorization

Given Carlo is not a Security operator in ProTego

When Carlo checks if there are changes in the risk assessment

Then Carlo should be notified that he cannot review new evaluations

Scenario: First-time risk assessment is still to be conducted

Given Andrew is a Security operator in ProTego

When Andrew checks if there are changes in the risk assessment

Then Andrew should be notified that the first-time risk assessment is still to be conducted

Table 102. Acceptance tests of the “Reflect infrastructure changes” use case

Scenario: Security operator reflects recent changes

Given The infrastructure and its risks are modeled into ProTego

And Andrew is a Security operator in ProTego

When Andrew provides an infrastructure model reflecting the current situation

Then Andrew should be made aware of possible new risks and mitigations actions

And ProTego should update the hospital infrastructure model and the associated risks

Scenario: Insufficient authorization

Given Carlo is not a Security operator in ProTego

When Carlo provides an infrastructure model reflecting the current situation

Then Carlo should be notified that he cannot reflect infrastructure changes

Scenario: First-time risk assessment is still to be conducted

Given Andrew is a Security operator in ProTego

When Andrew provides an infrastructure model reflecting the current situation

Then Andrew should be notified that the first-time risk assessment is still to be conducted

VIII.2. Non-functional success rate

The second metric we introduced is the *Non-functional success rate*, a comprehensive measurement calculated as the fraction of implemented acceptance criteria over the total amount of acceptance criteria presented from Table 104 to Table 106. The acceptance criteria themselves represent the expected outcome of a set of metrics that will measure non-functional qualities of ProTego such as the performance, and thus providing also an evaluation of a specific characteristic of the system.

The metrics have been identified following a process called goal-question-metric or GQM illustrated in Figure 11 [33]. The process starts by considering the business objectives that ProTego wants to achieve. For each objective, a series of questions have been defined as described in Table 103. Then, a set of metrics were specified to provide an answer to those questions, and therefore to judge if the objectives have been achieved. Moreover, the metric's acceptance criteria have been specified considering the research and development nature of the case studies of the project –FoodCoach and Pocket EHR. In a production environment, the metrics would be still valid, however their acceptance criteria should be recalibrated due to a higher degree of complexity of the system. In light of this consideration, the values of some of the acceptance criteria that are reported in Table 104, Table 105 and Table 106 have been defined in a looser way.

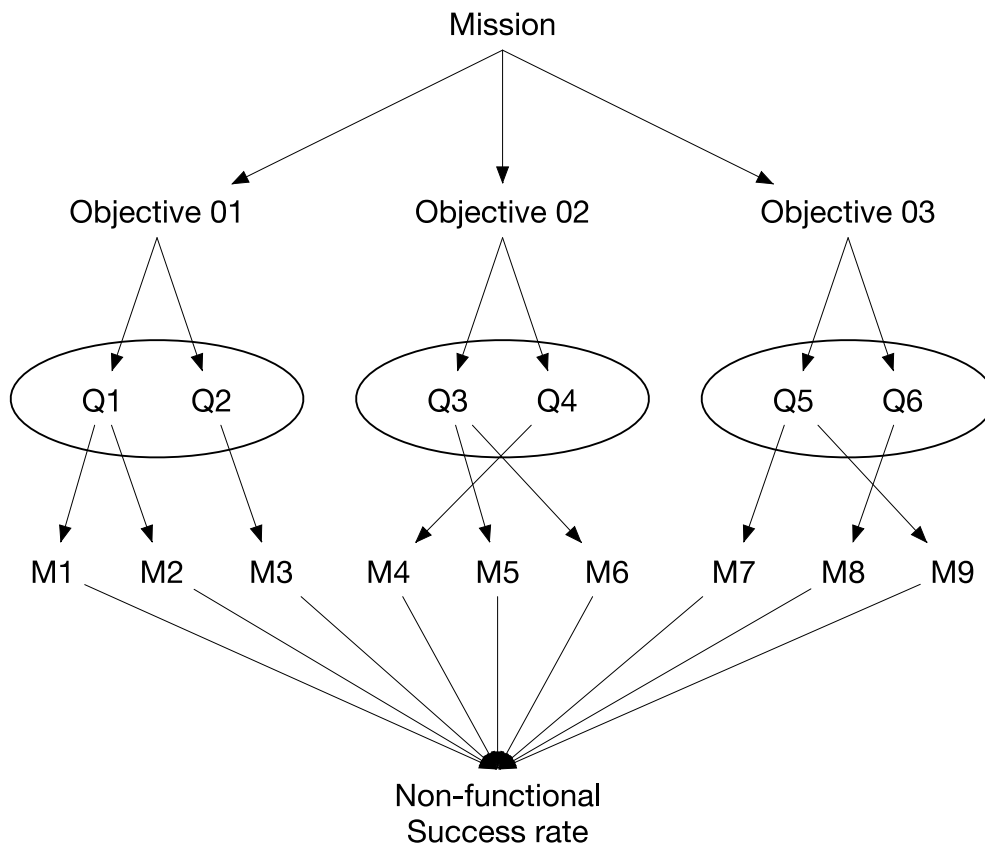


Figure 11. Goal-question-metric (GQM)

Table 103. Questions and Objectives

| ID | Question | Objective |
|-----|---|---|
| Q1 | <i>How effectively is situational awareness improved?</i> | "To improve situational awareness during an attack" |
| Q2 | <i>How efficiently does the system improve situational awareness during an attack?</i> | |
| Q3 | <i>Does the risk level increase as a result of new detected vulnerabilities?</i> | "To analyze and mitigate cybersecurity risk at design-time" |
| Q4 | <i>Does the risk level reduce as a result of the implemented mitigation strategies?</i> | |
| Q5 | <i>How effectively are data-at-rest protected?</i> | "To ensure end-to-end data protection" |
| Q6 | <i>How efficiently does the system perform with the data-at-rest protected?</i> | |
| Q7 | <i>How effectively are data-in-use protected?</i> | |
| Q8 | <i>How efficiently does the system perform with data-in-use protected?</i> | |
| Q9 | <i>How effectively are data-in-transit isolated?</i> | |
| Q10 | <i>How efficiently does the system perform with the data-in-transit isolated?</i> | |

One of the objectives that ProTego wants to achieve is *“To improve situational awareness during an attack”*. In order to evaluate the extent to which the objective has been achieved, the following questions have been posed:

Q1: How effectively is situational awareness improved?

Q2: How efficiently does the system improve situational awareness during an attack?

The first question has been addressed by defining a set of metrics aimed at measuring the type of alerts that are raised from those events that are considered to be significant in terms of security. With regard to the Access Control framework, several alerts can be raised. For example, it is meaningful to raise an alert about an invalid Authtoken, because it will make the operator aware of a potentially dangerous situation happening within the Access Control framework. In this fashion, the situational awareness is improved because the system will have the ability to promptly detect potential risks within the infrastructure. An alert can also be raised in those situations where the Access Control component receives a token that is faulty for one of the following reasons: its header is incorrect, its payload is incorrect, its data is in the wrong format, or the token is overall invalid. The occurrence of a single such an event is not necessarily the result of an attack, as an invalid token may be simply the result of a bug. Though, this is where the SIEM shows its value in improving situational awareness, as it is able to collect information from these alerts over a long period of time, which allows it to make inferences about what is going on. For example, multiple “Invalid Token” alerts over a certain period of time may indicate that an attacker is attempting to forge a token. Because the Continuous Authentication component is concerned with verifying whether the user’s behavior is trustworthy, this component can obviously raise an alert whenever such a condition is not met, that is, whenever the component believes that an attacker may be using the user’s mobile device. Lastly, as far as Network Slicing is concerned, two types of alerts can be raised: one to warn about malicious scans and the other about anomalous traffic. More specifically, the former is useful in discovering ongoing scans, which could imply that someone may be performing a malicious scan on an access point to find all its open ports, and, possibly, a vulnerable service. On the other hand, the latter is useful to detect network activity that is deemed suspicious according to a set of pre-defined rules.

The second question has been tackled by describing a set of metrics that measure the expected performance of the system in order to improve situational awareness. The first metric that we introduced is the Event collection rate. It expresses the number of collected events within a given timeframe, and it was defined with a value that is considered suitable so as not to cause a congestion. Another metric that we introduced is the Event processing rate. An appropriate value for this metric depends a lot on the resources allocated (CPU and RAM), number of agents, and events per agent so that the resources are not overloaded. Total log storage describes the total amount of logs stored. This measurement is relevant because it influences the number of resources required to sustain the SIEM, given an average number of alerts per seconds and the number of agents installed. Additionally, the Log source count describes the number of log sources analyzed by the SIEM. The acceptance criteria of this metric include all the log sources of the ProTego infrastructure. Lastly, we introduced the Resource usage as a metric to describe the resources necessary to utilize the SIEM.

The achievement of the metrics reported in Table 104 collectively contribute to the achievement of a satisfactory level of “Mean-Time-To-Detect” and “Mean-Time-To-Respond” when addressing the most significant security-related events. These are two key qualities to enhance the hospital’s security capabilities.

Table 104. Metrics to evaluate the situational awareness

| Questions | Component | Metric | Description | Acceptance criteria |
|--|-----------------|--|--|---|
| Q1: How effectively is situational awareness improved? | SIEM | Access control alerts | It describes an alert raised when the Data Gateway's "Authtoken" is not valid | Alert raised from Invalid Authtoken |
| | | | It describes an alert raised when the Access Control verifies that signature has expired | Alert raised from Token signature expired |
| | | | It describes an alert raised when the Access Control verifies that the token is invalid | Alert raised from Invalid token |
| | | | It describes an alert raised when the token type is neither "Keycloak" nor "AWS-cognito" | Alert raised from Wrong token type |
| | | | It describes an alert raised when the unwrapped key is not in the base64 encoded format | Alert raised from Wrong data format |
| | | | It describes an alert raised when the header structure is not correct | Alert raised from Incorrect header |
| | | | It describes an alert raised when the payload structure is not correct | Alert raised from Incorrect payload structure |
| | SIEM | Continuous authentication alerts | It describes an alert raised when the trust of the user's identity drops below a threshold | Alert raised from Untrusted user value |
| | SIEM | Data gateway alerts | It describes an alert raised when a cryptographic problem is detected when trying to read a Parquet file | Alert raised from Bad key |
| | SIEM | Network Slicing | It describes an alert raised when a user tries to perform a malicious scan on an access point | Alert raised from malicious scans |
| SIEM | Network Slicing | It describes an alert raised when the traffic coming from a user or an | Alert raised from anomalous traffic | |

| | | | | |
|---|------|------------------------|--|--|
| | | | access point is anomalous | |
| Q2: How efficiently does the system improve situational awareness during an attack? | SIEM | Event collection rate | It describes the number of collected events within a given timeframe | 500 Events/Second per Agent |
| | SIEM | Event processing rate | It describes the number of processed events within a given timeframe | This value depends a lot on the resources allocated (CPU and RAM), number of agents, and events per agent. |
| | SIEM | Total log storage | It describes the total amount of logs stored | For 100 agents, 80GB/month |
| | SIEM | Log source count | It describes the number of log sources analyzed | <ul style="list-style-type: none"> • Application • Data Gateway • Access control • Network slicing • Continuous authentication • SSM • System logs • Network devices |
| | SIEM | Alerts triggered count | It describes the number of alerts raised within a given timeframe | This value can only be calculated after the SIEM has been working for a time |
| | SIEM | Resource usage | It describes the resources necessary to utilize the SIEM | CPU: 8 cores RAM: 16 GB Disk: 5 GB |

The second objective that ProTego wants to achieve is “*To analyze and mitigate cybersecurity risk at design-time*”. In order to evaluate the extent to which the objective has been achieved, the following questions have been posed:

Q3: Does the risk level increase as a result of new detected vulnerabilities?

Q4: Does the risk level reduce as a result of the implemented mitigation strategies?

The specified questions are addressed through the “risk vector” metric that expresses the level of risk detected in the system. This metric will be measured in an empirical way by performing dynamic trials. In the first trials, the vulnerabilities will be deliberately injected into the system. In this way the system should report an increase of the risk level in response to the detection of such vulnerabilities. In the second trial, the recommendations made by the SSM to reduce the overall risk level will be implemented, so that the system should report a decrease of the risk level.

The risk vector is a sequence of five values each expressing the number of risks using a severity scale, that goes from very low to very high. A risk vector, can be expressed with the following formula: $RV = [vl, l, m, h, vh]$ where **vl** is the number of very low risks, **l** is the number of low risks, **m** is the number of medium risks, **h** is the number of high risks and **vh** is the number of very high risks. Two examples of such a vector are vector1 = [26,65,35,23,0] and vector2 = [12,45,56,0,0], where vector1(high risk) expresses a risk level higher than vector2 (medium risk). These examples illustrate how a raised risk means larger numbers in the higher-level risk levels, and a reduced risk means smaller or zero numbers in the higher-level risks. The proposed empirical trials provide an effective way to measure the extent to which ProTego is capable of detecting and mitigating risks within the hospital infrastructure.

Table 105. Metrics to evaluate risk detection and mitigation

| Questions | Component | Metric | Description | Acceptance criteria |
|---|------------|--------------------------------|--|---|
| Q3: Is the risk level increased as a result of new detected vulnerabilities? | SIEM / SSM | Increase of risk vector level | Risk level increase in response to a deliberate vulnerability injected into the system | SIEM should detect vulnerability. Overall risk level should increase as a result of the vulnerability being injected |
| Q4: Is the risk level reduced as a result of the implemented mitigation strategies? | SSM | Reduction of risk vector level | Risk level reduction in response to mitigating control recommendations to address a detected vulnerability | Overall risk level should reduce from the risk level when vulnerability was injected as a result of the recommendations made by the SSM |

The third objective that ProTego wants to achieve is “*To ensure end-to-end data protection*”. In order to evaluate the extent to which the objective has been achieved, the following questions have been posed:

Q5: How effectively are data-at-rest protected?

Q6: How efficiently does the system perform with the data-at-rest protected?

Q7: How effectively are data-in-use protected?

Q8: How efficiently does the system perform with data-in-use protected?

Q9: How effectively are data-in-transit isolated?

Q10: How efficiently does the system perform with the data-in-transit isolated?

Q5 has been addressed specifying the AES key size of the Data Gateway. It is important to provide a long key to ensure data protection. Indeed, the longer the key is, the more difficult it becomes to brute-force it and break the cryptographic scheme. Moreover, it is important to balance the necessity to protect data without compromising the performance of the system (Q6). Therefore, two metrics have been specified to measure the impact on the performance during the writing and the reading of the data.

In order to respond to how effectively data-in-use are protected (Q7), a set of metrics have been specified. Concerning the Access Control framework, the hospital's use cases need to utilize RBAC (Role Based Access Control). Because of that, the number of user roles supported must be equal to the number of categories of application users. As in the case of Data Gateway, the length of the key for the Access Control framework is a determining factor to ensure data protection, and a length of at least 128-bit is considered to be sufficient. Moreover, a low value of the False Acceptance Rate (FAR) and of the False Rejection Rate (FRR) is fundamental to prevent unauthorized access and therefore ensure data protection. Reducing the FAR to the lowest possible level, the FRR is likely to rise sharply so that it is important to strike a balance between the FAR and FRR to prevent unauthorized access while not falsely rejecting legitimate users. The FAR and the FRR have been used also to evaluate the effectiveness of the Continuous Authentication mechanism –considering its own values as acceptance criteria. The description of the accuracy and the precision of the Continuous Authentication mechanism complete the specification of those values to be measured in order to respond to how effectively data-in-use are protected. A high accuracy guarantees that the system is able to classify both authorized and unauthorized accesses correctly. A high Precision guarantees that legitimate accesses are still correctly classified.

The communication overhead of the Access Control framework is the main factor that impacts the efficiency of the system, while protecting data-in-use (Q8). Each access requests triggers a communication flow, in which the data consumer needs to connect to the data gateway and to the access control framework, to send the required information. The more bits that need to be sent to the access control framework, the higher the complexity. Therefore, the communication overhead induced by the Access Control solution should be as limited as possible.

In order to establish how effectively data-in-transit are isolated (Q9) the number of slices has been defined as a metric for the Network Slicing component. Increasing the number of slices, on the one hand increases the degree of isolation and customization of the network traffic, but on the other hand it reduces the throughput of each slice. For this reason, the resulting number of slices has been defined according to the number of user type to ensure the proper level of isolation without compromising the capacity.

Moving on to the data-in-transit efficiency (Q10), the throughput determines how much data can be transferred from source to destination within a given timeframe. A high value of throughput

determines a higher quality of the service, while a low value of throughput could compromise the availability in health services. Another performance indicator is the latency which drives the responsiveness of the network. High latency would compromise the availability in health services, so it is important to ensure that its value is as low as possible. The packet loss is an additional metric to be considered since it is relevant for the quality of the service. A high percentage of packet loss would compromise the integrity of data in transit within the hospital network. The last metric is the VPN additional delay, which expresses the overhead caused by the encryption and decryption of the data flow in the VPN tunnel. This value should be the lowest possible.

Overall, the metrics reported in Table 106 will serve as a way to evaluate the improvement of the security of applications, data and infrastructure, and therefore reducing the risk of data privacy breaches.

Table 106. Metrics to evaluate end-to-end data protection

| Questions | Component | Metric | Description | Acceptance criteria |
|--|---------------------------|----------------------------------|--|---|
| Q5: How effectively are data-at-rest protected? | Data Gateway | AES key size | It describes the number of bits in a key used by a cryptographic algorithm. | At least 128-bit |
| Q6: How efficiently does the system perform with the data-at-rest protected? | Data Gateway | Writing overhead | It describes the ratio between performing write operations on encrypted data and unencrypted data | MAX +11% time |
| | Data Gateway | Reading overhead | It describes the ratio between performing read operations on encrypted data and unencrypted data | MAX +65% time |
| Q7: How effectively are data-in-use protected? | Access control | False Acceptance Rate (FAR) | It measures the percentage of identification instances in which unauthorized persons are incorrectly accepted. | $FAR < 10^{-6}$ |
| | Access control | False Rejection Rate (FRR) | It measures the percentage of identification instances in which authorized persons are incorrectly rejected. | $FRR < 10^{-3}$ |
| | Access control | Access control type | It describes the granularity of access control policies that can be applied. | At least RBAC (Role Based Access Control) |
| | Access control | Number of user roles supported | It measures the number of user roles that the system support | At least two roles (doctor + patient) |
| | Access control | Security strength of key storage | It is the number of bits in a key used by a cryptographic algorithm | At least 128-bit security |
| | Continuous Authentication | False Acceptance Rate (FAR) | It measures the percentage of identification instances in which unauthorized persons are incorrectly accepted. | $FAR < 0.5\%$ |

| | | | | |
|---|---------------------------|---|---|--|
| | Continuous Authentication | False Rejection Rate (FRR) | It measures the percentage of identification instances in which authorized persons are incorrectly rejected. | FRR < 2% |
| | Continuous Authentication | Accuracy | It measures the proportion of true positives and negatives to the overall tested data | Accuracy > 98% |
| | Continuous Authentication | Precision | It expresses how frequently the system correctly produces positive classifications. It is calculated as the ratio of true positive to both true and false positive | Precision > 95% |
| Q8: How efficiently does the system perform with data-in-use protected? | Access control | Communication overhead per access request | The number of bits (specifically related to the access control solution) that need to be sent to the access control framework by a data consumer in order to access a specific resource | MAX 1 KB |
| | Access control | Number of IAMs supported | It is the number of identity and access management solutions supported in the access control system | At least 1 IAM supported per hospital within ProTego |
| Q9: How effectively are data-in-transit isolated? | Network slicing | Number of slices | It is the maximum number of slices supported in the wireless segment. Inside each slice one or more clients can send traffic from one or more applications | At least 3 slices |
| Q10: How efficiently does the system perform with the data-in-transit isolated? | Network slicing | Throughput per VPN tunnel | Throughput per VPN tunnel refers to how much data can be transferred from source to destination within a given timeframe for each slice. | Min 100 Mbps |
| | Network slicing | Latency | It drives the responsiveness of the network that is how fast each conversation can be had. It is measured as the total round-trip time it takes for a data packet to travel. Latency also drives the maximum throughput of a conversation | Max 5 ms |
| | Network slicing | Throughput | It refers to how much data can be transferred from source to destination within a given timeframe. | Min 10 Mbps |

| | | | | |
|--|-----------------|----------------------|--|------------|
| | Network slicing | Packet loss | It is measured as a percentage of packets lost with respect to packets sent. | Max 0.001% |
| | Network slicing | VPN additional delay | It is the extra communication delay caused by the encryption/decryption of the data flow in the VPN tunnel | Max 0.7 ms |

VIII.3. Usability metrics

According to [30], *Usability* is the extent to which a system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. As the definition suggests, we measure usability in terms of three metrics: (i) *Effectiveness*, that is, the ability to complete a task; (ii) *Efficiency*, that is, the amount of effort required to complete the task and (iii) *Satisfaction*, that is, the degree to which the user is happy with his or her experience while performing the task.

Such metrics will be determined by means of a *Usability test*, which allows evaluating the user interaction as a combination of measurable traits (error frequency, time per task, etc.), and self-reported feedback from the participants. More specifically, the usability test proceeds as follows:

1. **Use case scenario assessment.** The participant is asked to perform a certain use case scenario of Table 107. During the test, the usability team records relevant aspects of the user interaction (errors, time per task, etc.) that determine the system *effectiveness* and *efficiency*. Moreover, the usability team collects any qualitative feedback (what the participant thinks out loud) concerning the performed scenario.

2. **After-Scenario Questionnaire.** The usability team administers to the participant the *After-Scenario Questionnaire* (ASQ) [31]. The questionnaire consists of the following three statements:

Q1 “*I am satisfied with the ease of completing the tasks in this scenario.*”

Q2 “*I am satisfied with the amount of time it took to complete the tasks in this scenario.*”

Q3 “*I am satisfied with the support information (online help, messages, documentation) when completing the tasks.*”

where each statement is accompanied by a 7-point rating scale, from “strongly disagree” to “strongly agree,” as shown in Figure 6.1. The questionnaire touches on all the usability metrics: effectiveness (Q1), efficiency (Q2), and satisfaction (Q1, Q2, Q3).

3. **System Usability Scale (SUS).** The usability team administers to the participant the *System Usability Scale* (SUS) [32]. The questionnaire consists of ten statements, half of which are positively worded and half negatively worded. Each statement is accompanied by a 5-point scale of agreement (Figure 13). The usability team combines the ten ratings into an overall usability score, on a scale of 0 to 100.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------|
| 1. Overall, I am satisfied with the ease of completing the tasks in this scenario ☐ | strongly disagree | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | strongly agree |
| 2. Overall, I am satisfied with the amount of time it took to complete the tasks in this scenario ☐ | strongly disagree | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | strongly agree |
| 3. Overall, I am satisfied with the support information (online-line help, messages, documentation) when completing the tasks ☐ | strongly disagree | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | strongly agree |

Figure 12. After-Scenario Questionnaire (ASQ) administered via a Web interface

| | Strongly disagree | | | | | Strongly agree |
|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|----------------|
| 1. I think that I would like to use this system frequently. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 4 |
| 2. I found the system unnecessarily complex. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 1 |
| 3. I thought the system was easy to use. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1 |
| 4. I think I would need the support of a technical person to be able to use this system. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 4 |
| 5. I found the various functions in this system were well integrated. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1 |
| 6. I thought this system was too inconsistent. | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 2 |
| 7. I would imagine that most people would learn to use this system very quickly. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1 |
| 8. I found the system very cumbersome to use. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 1 |
| 9. I felt very confident using the system. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 4 |
| 10. I needed to learn a lot of things before I could get going with this system. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 3 |

Figure 13. System Usability Scale (SUS)

As mentioned, the usability test for ProTego focus on testing the use cases presented in Section III.4. – including the provisioning of the environment and installation of the ProTego toolkit. Table 107 illustrates the use cases, and the related actors, that will be involved in the study.

Table 107. Use cases that are going to be tested during the usability test

| ID | Use case | Actor |
|------|--|-------------------|
| UC01 | Deploy cluster | System Operator |
| UC02 | Install Data Gateway | System Operator |
| UC03 | Install Network Slicing | System Operator |
| UC04 | Install SIEM | System Operator |
| UC05 | Install SSM | System Operator |
| UC06 | Install Continuous authentication | System Operator |
| UC08 | Conduct first-time risk assessment | Security operator |
| UC09 | Assess prospective risks to the infrastructure | Security operator |
| UC10 | Install application | System operator |
| UC11 | Configure application network slices | Network operator |
| UC12 | Configure application logging mechanism | Security operator |
| UC13 | Specify application access control | Security operator |
| UC14 | Configure mobile device | Security operator |
| UC15 | Store initial medical data | Data operator |
| UC16 | Register mobile device | Network operator |
| UC23 | Respond to alert | Security operator |
| UC24 | Review alerts | Security operator |
| UC25 | Review new risk evaluation | Security operator |
| UC26 | Reflect infrastructure changes | Security operator |

IX. Conclusions

In this document, we presented the final specification of the ProTego requirements. In line to what discussed in the Description of the Action, we provided an analysis of the ProTego solution in terms of its stakeholders, objectives and expected outcomes. We further commented on the features that are going to enable such impacts, thus determining the scope of the final release of the project software solution. On top of that, we presented a set of use cases detailing the interactions between the system and its relevant user classes. Then, we moved to the presentation of the two project case studies. Each case study has been analyzed in terms of its stakeholders, users, and detailed uses cases. The applications presented in each case study will interact with the hospital infrastructure by means of ProTego, therefore acting as the demonstration platform of the project. In this context, we presented a selection of representative real-life situations in the life of patients in which their safety and privacy, as well as the infrastructure itself may be put at risk, commenting on how ProTego can assist in reducing such a risk. Finally, we include the final description of the metrics useful for the assessment of the achieved solution.

X. References and Internet Links

- [1] H. Thimbleby, "Technology and the future of healthcare," in *Journal of public health research*, 2013, 2.3.
- [2] A. Boddy, et al. "A study into detecting anomalous behaviours within healthcare infrastructures," in *9th International Conference on Developments in eSystems Engineering*, 2016.
- [3] M.S. Jalali, and J. P. Kaiser, "Cybersecurity in hospitals: a systematic, organizational perspective," in *Journal of medical Internet research*, 2018.
- [4] L. Coventry, and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," in *Maturitas*, 2018, 113:48-52.
- [5] S. Morgan, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," *Cybersecurity Ventures* [Website]. Available: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>
- [6] Symantec, "Cybersecurity in Healthcare: Why It's Not Enough, Why It Can't Wait," *Symantec* [Website]. Available: <https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf>
- [7] J. M. Ehrenfeld, "Wannacry, cybersecurity and health information technology: A time to act," in *Journal of medical systems*, 2017, 41.7: 104.
- [8] J. Fruhlinger, "What is WannaCry ransomware, how does it infect, and who was responsible?," *CSO Online* [Website]. Available: <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>
- [9] S. T. Argaw, et al, "The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review," *BMC medical informatics and decision making*, 2019,19.1: 10.
- [10] Cisco, "Healthcare Security: Improving Network Defenses While Serving Patients," *Cisco* [Website]. Available: <https://www.cisco.com/c/dam/en/us/products/collateral/security/security-benchmark.pdf>
- [11] I. Alexander, "Stakeholders: who is your system for?," in *Computing and Control Engineering*, 2003, 14.2: 22-26.
- [12] I. Alexander, and S. Robertson, "Understanding project sociology by modeling stakeholders," *IEEE Software* 21.1, 2004, 23-27.
- [13] A. Kossiakoff et al., "Systems engineering: Principles and Practices," John Wiley & Sons, Inc., 2003.
- [14] M. Fowler, and C. Kobryn, "UML distilled: a brief guide to the standard object modeling language," Addison-Wesley Professional, 2004.
- [15] A. Chen, and J. Beatty, "Visual models for software requirements," Pearson Education, 2012.
- [16] K. Wiegers, and J. Beatty, "Software requirements," Pearson Education, 2013.
- [17] A. Cockburn, "Writing effective use cases," Addison-Wesley Professional, 2000.
- [18] S. Robertson, and J. Robertson, "Mastering the requirements process: Getting requirements right," Addison-Wesley, 2012.
- [19] A. Cooper, "The inmates are running the asylum: Why high-tech products drive us crazy and how to restore the sanity," Sams - Pearson Education, 2004.

- [20] I. Alexander, and N. Maiden, "Scenarios, stories, use cases: through the systems development life-cycle," John Wiley & Sons, 2005.
- [21] ISO/IEC, "ISO/IEC 25010: 2011 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models," 2011.
- [22] S. Mark, "Information Security: Principles and Practice," John Wiley & Sons, 2011.
- [23] A. Mavin et al. "Easy approach to requirements syntax (EARS)." *In 17th IEEE International Requirements Engineering Conference*, 2009.
- [24] D. Firesmith, "Engineering security requirements," in *Journal of object technology*, 2003, 2.1: 53-68.
- [25] European Parliament and The Council, "General Data Protection Regulation." Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>
- [26] A. Shostack, "Threat modeling: Designing for security," John Wiley & Sons, 2014.
- [27] K. Pugh, "Lean-Agile Acceptance Test-Driven Development: Better Software Through Collaboration," Addison-Wesley, 2011.
- [28] D. North, "Introducing BDD," Dan North & Associates. Available: <https://dannorth.net/introducing-bdd/>
- [29] K. Nicieja, "Writing Great Specifications: Using Specification by Example and Gherkin," Manning Publications, 2017.
- [30] International Organization for Standardization. "ISO 9241-11: 2018, Ergonomics of human-system interaction-Part 11: Usability: Definitions and concepts." ISO standards catalogue, 2018.
- [31] J. R. Lewis, "Psychometric evaluation of an after-scenario questionnaire for computer usability studies: the ASQ." *SIGCHI Bull.* 23, 1, 1991.
- [32] J. Brooke, "System usability scale (SUS): a quick-and-dirty method of system evaluation user information." Reading, UK: Digital Equipment Co Ltd 43, 1986
- [33] R. Van Solingen, E. Berghout, "The Goal/Question/Metric Method. A practical guide for quality improvement of software development." McGraw-Hill Publishing Company, 1999



ProTego