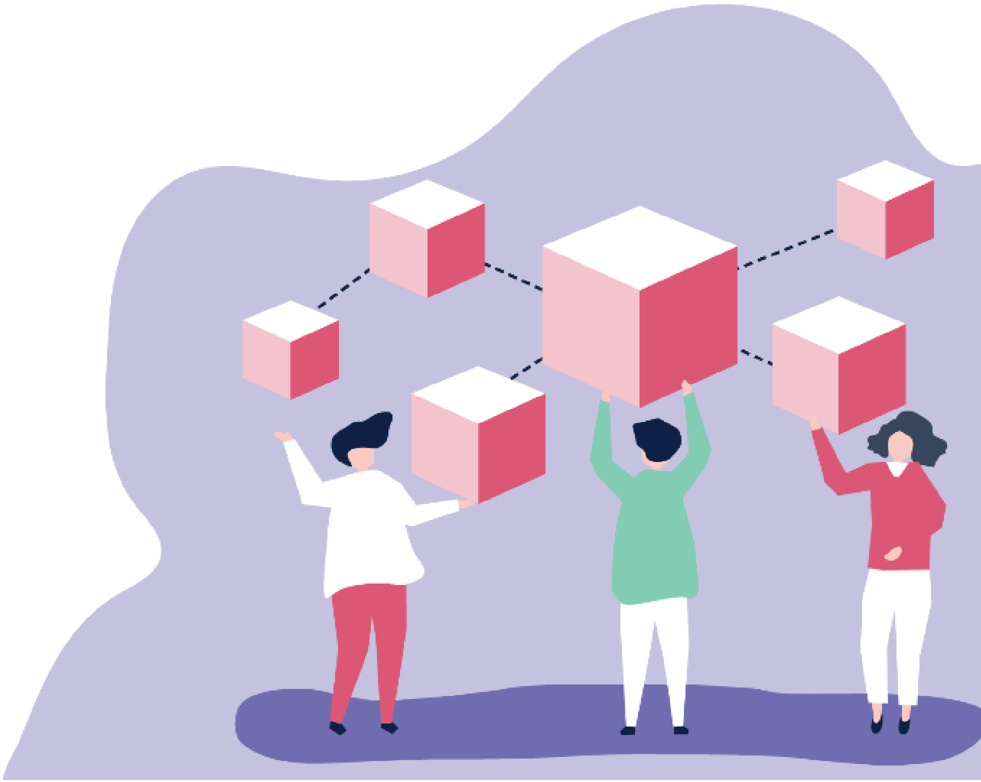
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223

GATE KEEPER

D2.6.2 Open call report

Deliverable No.	D2.6.2	**Due Date**	30/09/2021
Description	Open call. Guide for applicant		
Type	Report	**Dissemination Level**	PU
Work Package No.	WP2	**Work Package Title**	Eco-system value co-creation, Open Calls and scaling up twinning
Version	1.0	**Status**	Final



Authors

Name and surname	Partner name	e-mail
Marta Perez	Medtronic	Marta.perezalba@medtronic.com
Eugenio Gaeta	UPM	eugenio.gaeta@lst.tfo.upm.es
Silvio Pagliara	UoW	Silvio. pagliara@warwick.ac.uk
Leandro Pecchia	UoW	l.pecchia@warwick.ac.uk
Lidia Manero	Medtronic	Lidia.manero.mijangos@medtronic.com

History

Date	Version	Change
01/07/2021	0.1	Draft version
15/09/2021	0.2	Contributions added
22/09/2021	0.3	Final Version ready for peer review
29/09/2021	0.4	Peer review by Tecnalia
30/09/2021	0.5	Peer review by ECHA

Key data

Keywords	Open call, proposal, evaluation
Lead Editor	Marta Perez
Internal Reviewer(s)	Leire Bastida (Tecnalia); Karolina Mackiewicz (ECHA)

Abstract

This document provides a complete overview and results of the first open call. In this document the publication of the call, evaluation criteria and selected proposals are presented.

This deliverable also identifies and discusses best practices, which were useful to run GATEKEEPER open calls for recruiting third parties to extend and exploit the GATEKEEPER ecosystem.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Table of contents

List of tables

List of figures

1 Introduction

1.1 Overview open call activity

The GATEKEEPER project currently active under H2020 Framework Programme of the European Commission offers the opportunity to third parties to contribute in the development and sustainability of the project and get financially supported after its selection via open call on the basis of the submitted proposals.

The Open Call is one of the important means towards exploitation and verification of the GATEKEEPER architecture and developed technologies. Moreover, through Open Calls the project aims at widening the GATEKEEPER ecosystem by involving new partners and enhancing the offerings of the GATEKEEPER marketplace. The GATEKEEPER project use the Open Calls as one of the key tools to impact and attract new stakeholders around the ecosystem, and to consolidate the stakeholders' relationships and roles inside the ecosystem.

One of the main expected impact of the GATEKEEPER project is to ignite the market growth and future sustainability of the ecosystem, extending the benefits of GATEKEEPER experience beyond the boundaries of current pilots, from new cities and regions deploying digital services in Health and care through GATEKEEPER ecosystem, to new SMEs designing new innovative applications and technologies, and to new users and beneficiaries.

According to this, the GATEKEEPER project organized two different open calls:

- First Open Call - planned for M14, with a total budget of 600.000€, is focused on implement new AI and Big Data applications, tools or components in the platform
- Second Open Call - planned for M23, with a total budget of 600.000€, is addressed to cities and regions in the EU that are willing and committed to set up GATEKEEPER platform for digital services in healthcare and in their local ambit and commit the contribution in the evaluation and evidence creation process of gatekeeper as well the sustainability and growth beyond the end of the project.

The timeline of the task 2.5 "Definition, coordination & evaluation of Open Call Activities" for Open Call 1 is mentioned in Figure 2.

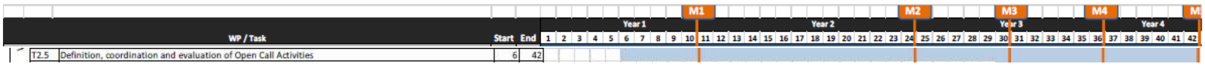


Figure 1. Timeline Task Open call activities

-

The Requirements for the First Open Call are documented in the deliverable D2.1 "initial ecosystem Management (M15). These requirements were included in the "Guide for applicants1", to orientate the content of proposals accordingly to the project's needs.

The first Open Call was open to Industries, SMEs, start up, Universities and research and technical centres registered in a member state of the European Union willing to implement innovative AI solutions within the GATEKEEPER ecosystem. The projects should have an implementation period of 12 months and not have more than 60.000€ of budget. The expected number of funded projects was 80

The first Open Call was conducted following the basic principles that govern Commission calls and are provided in the "Guidance note on financial support to third parties under H20202": excellence of selected proposals, transparency, fairness and impartiality, confidentiality, efficiency and speed of evaluation.

The next sections describe the activities related to the Open Call, from the preparation until the outcome

2 Dissemination

The main goal of an open call is to create impact and start to create a community behind the project. To disseminate to the widest possible communities, several activities to achieve this goal are detailed below.

2.1 Preparation

A dedicated section of the GATEKEEPER website[1] for the promotion of the Open Call has been prepared as well as an application form in Submitsquare[2], a standard tool for applications. Following documents (included in the Annexes of this document) have been prepared and published on the website:

- **Guide for applicants**: a description of the project, the open call goals and the whole open call procedure, as well the eligibility criteria and the evaluation criteria.
- **Applicant template:** to be filled by participants.
- **Technical information**: clarifications about GATEKEEPER
- **Template:** to be filled in by participants.
- **Third party agreement**: a draft of the agreement that winning proposers have to sign with the GATEKEEPER legal entity

The preparation activities also included search for the evaluators who assessed received proposals. All partners of GATEKEEPER consortium were invited to propose independent evaluators. More than 30 candidates were identified and their availability for the evaluation period had been checked.

2.2 Promotion

The main goal of the Open Call campaign was to create awareness of this funding opportunity attracting potential beneficiaries using the GATEKEEPER digital channels. The target audiences were mainly start-ups and SMEs interested on incorporating their technologies in the existing pilots. The purpose was not only to achieve their participation on the Open Call but also to create a dialogue with these organizations for enlarging the GATEKEEPER community.

The promotion campaign was designed and largely executed by Medtronic with the support of the D&C working group at local level and the AG08 included of the Large Scale

[1] https://www.gatekeeper-project.eu/1st-gk-open-call

[2] https://gatekeeper.submitsquare.com/#/calls/1

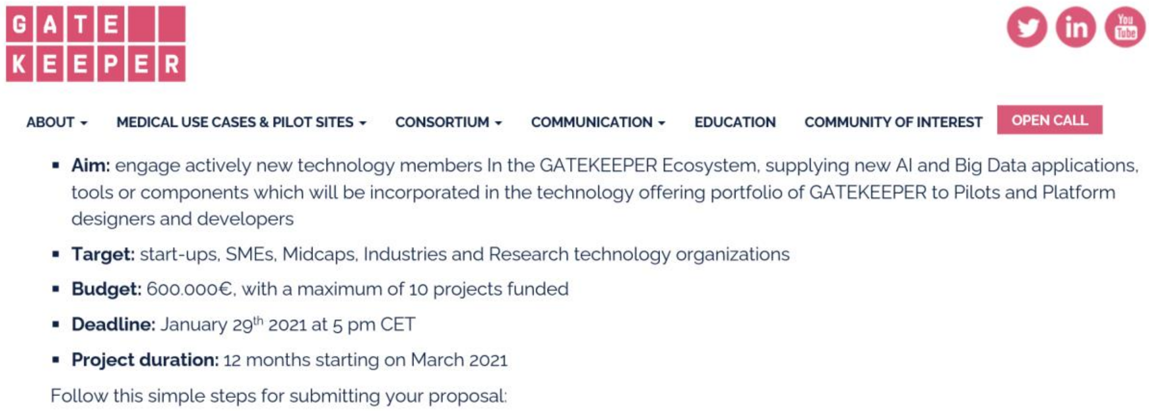
Pilot Program. In this respect, Medtronic created a toolkit including several materials with key messages and a common branding that was shared with those groups for multiplying the OC scope among their networks.

Following actions were put in place to accomplish with the scope expressed above:

2.2.1 Web

This channel was the main point of information for the open call participants. Before the launching, the Open Call (OC) section summarized the main info as following:

- Aim
- Target
- Budget
- Deadline
- Project duration



- **Aim:** engage actively new technology members In the GATEKEEPER Ecosystem, supplying new AI and Big Data applications, tools or components which will be incorporated in the technology offering portfolio of GATEKEEPER to Pilots and Platform designers and developers
- **Target:** start-ups, SMEs, Midcaps, Industries and Research technology organizations
- **Budget:** 600.000€, with a maximum of 10 projects funded
- **Deadline:** January 29th 2021 at 5 pm CET
- **Project duration:** 12 months starting on March 2021

Follow this simple steps for submitting your proposal:

Figure 2. Information posted on the main website

The official launching was on 31st October. On this date a simple three steps process was available for the users:

1. **Registration.**

By providing their contact details users were able to jump to the second point and obtaining all the OC documentation.

This registration process was stablished for two main purposes; from one side to control the interest produced by the OC tracking the numbers for users registered and in the other hand to create the OC database for sending relevant info regarding the OC and/or future collaborative opportunities.

2. **Documentation**

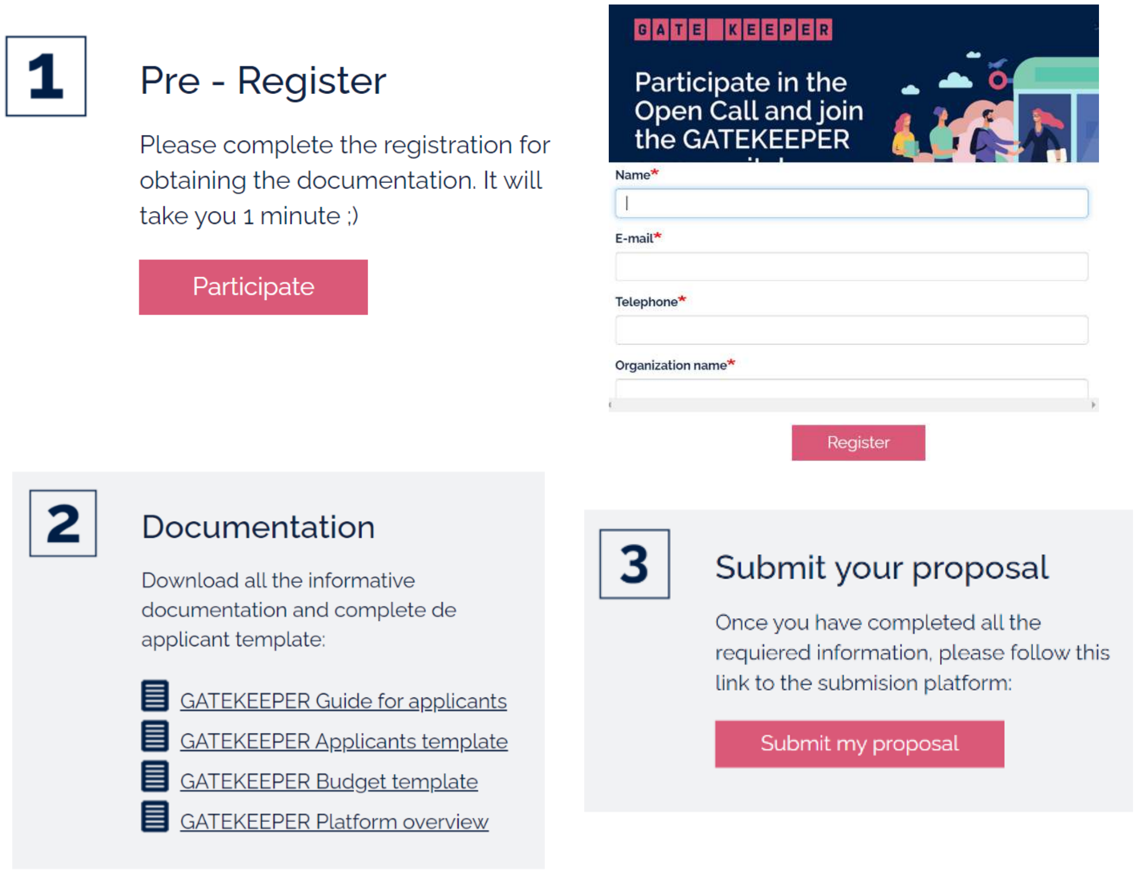
A four documents catalogue were created for the participants. Relevant information about the call and how to apply were described as follow:

- **Guide for applicants:** a description of the project, the open call goals and the whole open call procedure, as well the eligibility criteria and the evaluation criteria.
- **Technical information:** clarifications about GATEKEEPER
- **Template:** to be filled in by participants.

- **Third party agreement:** a draft of the agreement that winning proposers must sign with the GATEKEEPER legal entity

3- Proposal submission

After completing all the required documentation following the instructions, the link to the submittable portal was included in step 3.



1

Pre - Register

Please complete the registration for obtaining the documentation. It will take you 1 minute ;)

Participate

Participate in the Open Call and join the GATEKEEPER

Name*

E-mail*

Telephone*

Organization name*

Register

2

Documentation

Download all the informative documentation and complete de applicant template:

- GATEKEEPER Guide for applicants
- GATEKEEPER Applicants template
- GATEKEEPER Budget template
- GATEKEEPER Platform overview

3

Submit your proposal

Once you have completed all the requiered information, please follow this link to the submision platform:

Submit my proposal

To summarize, a specific section was created on the GATEKEEPER public website to feature as the main point of information regarding the Open Call. As indicated in the deliverable 9.1 Dissemination and Communication plan, a three-step process was available for the audiences to download all the required documentation needed to prepare a proposal. Thanks to this form, the GATEKEEPER database received more than 500 new contacts.

2.2.2 Social media

The Social Media channels, mainly Twitter and LinkedIn were used to boost the OC initiative. Moreover, a search of the main start-ups and accelerators in Europe was done for connecting and maintain them in the loop.

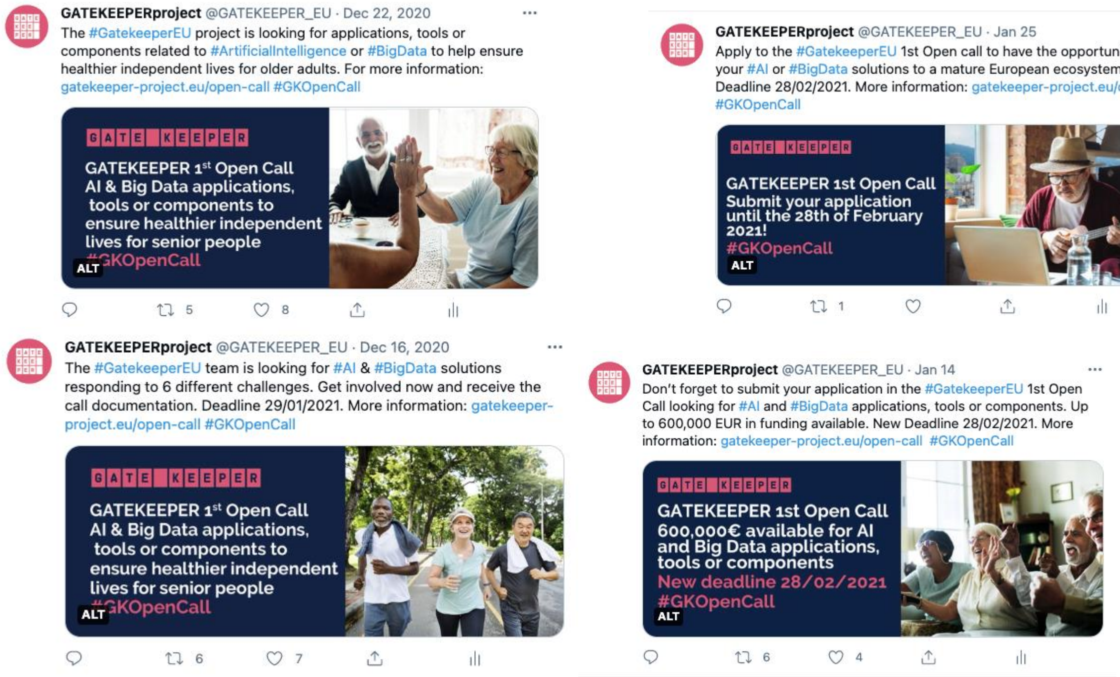
Twitter

Towards the end of 2020, a specific social media campaign was launched to promote the 1st Open Call of the GATEKEEPER project. The campaign was carried out from the 02.11.2020 until the 05.03.2021. The hashtag established for the campaign was #GKOpenCall.

The social media campaign consisted in 5 main phases:

1. Launch (02.11.2020 – 22.11.2020)
2. Sign up (23.11.2020 – 10.01.2021)
3. Deadline extension (11.01.2021 – 31.01.2021)
4. Final countdown to closure (01.02.2021 – 28.02.2021)
5. Follow-up (01.03.2021-05.03.2021)

A set of messages and accompanying visuals were designed and distributed to consortium members for each of the different phases of the campaign, adapting to changing needs, such as the deadline extension that was launched mid-January.



GATEKEEPERproject @GATEKEEPER_EU · Dec 22, 2020
The #GatekeeperEU project is looking for applications, tools or components related to #ArtificialIntelligence or #BigData to help ensure healthier independent lives for older adults. For more information: gatekeeper-project.eu/open-call #GKOpenCall

GATE KEEPER
GATEKEEPER 1st Open Call
AI & Big Data applications, tools or components to ensure healthier independent lives for senior people
#GKOpenCall
ALT
5
8

GATEKEEPERproject @GATEKEEPER_EU · Jan 25
Apply to the #GatekeeperEU 1st Open call to have the opportunity to offer your #AI or #BigData solutions to a mature European ecosystem. New Deadline 28/02/2021. More information: gatekeeper-project.eu/open-call #GKOpenCall

GATEKEEPERproject @GATEKEEPER_EU · Dec 16, 2020
The #GatekeeperEU team is looking for #AI & #BigData solutions responding to 6 different challenges. Get involved now and receive the call documentation. Deadline 29/01/2021. More information: gatekeeper-project.eu/open-call #GKOpenCall

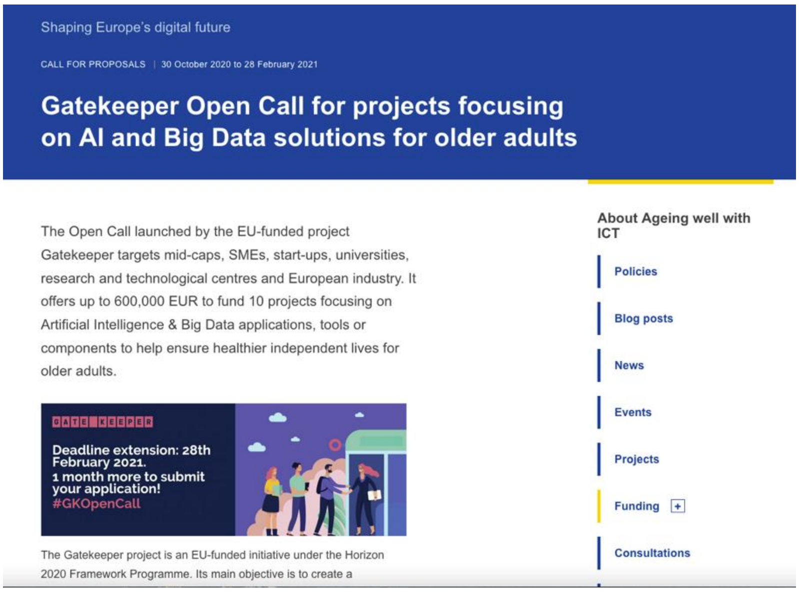
GATE KEEPER
GATEKEEPER 1st Open Call
AI & Big Data applications, tools or components to ensure healthier independent lives for senior people
#GKOpenCall
ALT
6
7

GATEKEEPERproject @GATEKEEPER_EU · Jan 14
Don't forget to submit your application in the #GatekeeperEU 1st Open Call looking for #AI and #BigData applications, tools or components. Up to 600,000 EUR in funding available. New Deadline 28/02/2021. More information: gatekeeper-project.eu/open-call #GKOpenCall

Figure 3. Examples of the visual images and accompanying messages developed for the campaign

Furthermore, the call was also published on various other websites, such as the Digital Single Market page of the European Commission[3]

[3] Full article: https://ec.europa.eu/digital-single-market/en/news/gatekeeper-open-call-projects-focusing-ai-and-big-data-solutions-older-adults



Shaping Europe's digital future

CALL FOR PROPOSALS | 30 October 2020 to 28 February 2021

Gatekeeper Open Call for projects focusing on AI and Big Data solutions for older adults

The Open Call launched by the EU-funded project Gatekeeper targets mid-caps, SMEs, start-ups, universities, research and technological centres and European industry. It offers up to 600,000 EUR to fund 10 projects focusing on Artificial Intelligence & Big Data applications, tools or components to help ensure healthier independent lives for older adults.

GATEKEEPER

Deadline extension: 28th February 2021.
1 month more to submit your application!
#GKOpenCall

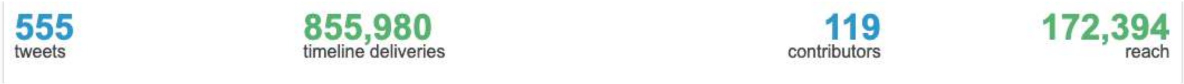
The Gatekeeper project is an EU-funded initiative under the Horizon 2020 Framework Programme. Its main objective is to create a

About Ageing well with ICT

- Policies
- Blog posts
- News
- Events
- Projects
- Funding +
- Consultations

Figure 4. The GATEKEEPER 1st Open call promoted on the European Commission's Digital Single Market Website

#GKOpenCall was used as the official hashtag for the 1st open Call. Figure 3 provides an overview of the Twitter activity using this hashtag. A total of 555 tweets were sent using this hashtag from 119 different people. The total number of timeline deliveries represents the total possible number of times someone could have viewed a particular tweet/post, in this case 855,980 times. The total reach represents the sum of all users mentioning your Twitter hashtag (#GKOpenCall) and the sum of their followers, in this case 172,394 users.



555 tweets

855,980 timeline deliveries

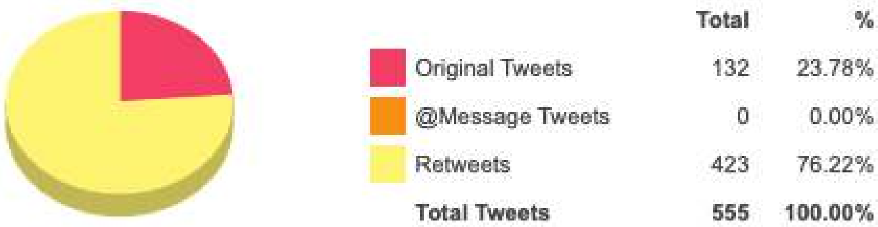
119 contributors

172,394 reach

Figure 5. Twitter activity using #GKOpenCAll hashtag

Continuing with an analysis of the overall Twitter activity for the 1st open call, the following figure shows the engagement using #GKOpenCall, which indicates whether the tweets sent were original tweets, message tweets or retweets. In this case, the figure below shows that the large majority of the Twitter activity was made up of retweets (423).

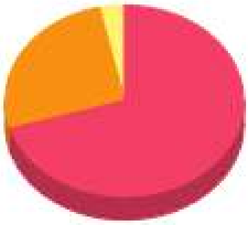
This figure suggests that the proposed messages were well defined and responded to the interest of the GATEKEEPER community and external stakeholders.



		Total	%
🟥	Original Tweets	132	23.78%
🟧	@Message Tweets	0	0.00%
🟨	Retweets	423	76.22%
	Total Tweets	**555**	**100.00%**

Figure 6 . Twitter engagement

The information in the chart titled participation highlights those people who were responsible for the majority of the tweets. It can be seen that a high amount of the tweets (390) were launched by the top 20 contributors.



		Total	%
🟥	From Top 20	390	70.27%
🟧	From Top 100	146	26.31%
🟨	The Rest	19	3.42%
	Total Tweets	**555**	**100.00%**

Figure 7 – Twitter participation

The Figure below lists the top additional hashtags that were used alongside the hashtag #GKOpenCall. This provides information on other relevant topics being communicated in connection with this campaign. From this list, we can see that many other subjects that are relevant to the gatekeeper project have been used such as #BigData and #ArtificialIntelligence.

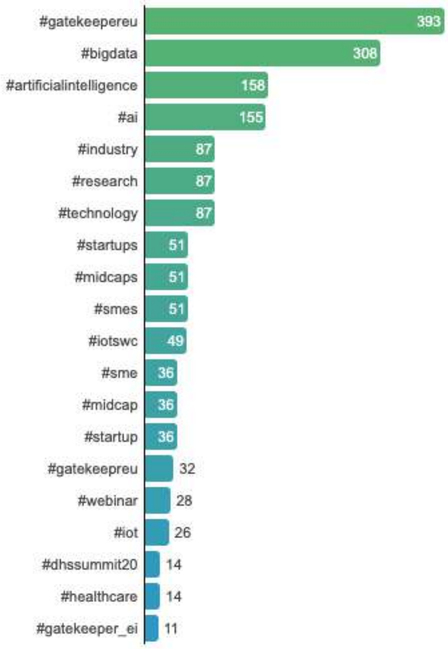


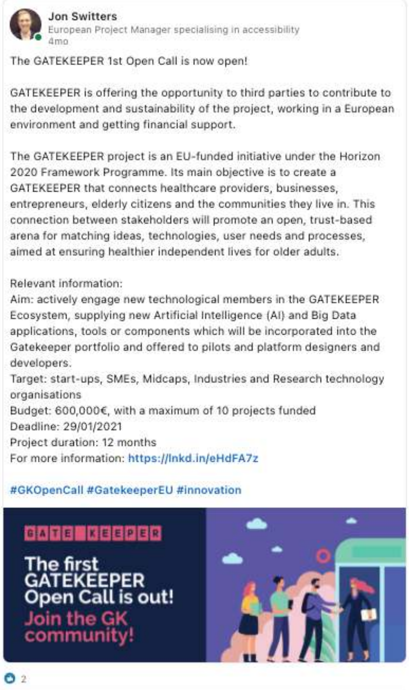
Figure 8. Top other hashtags

The following figure shows the Buzz words used in the tweets. Buzz words are the most popular words (not hashtags) that appeared in the tweets containing the #GKOpenCall.

Figure 9. Buzz words

LinkedIn

During the previously mentioned social media campaign for the GATEKEEPER 1st Open, Call, a set of messages were created for use on LinkedIn.



Jon Switters
European Project Manager specialising in accessibility
4mo

The GATEKEEPER 1st Open Call is now open!

GATEKEEPER is offering the opportunity to third parties to contribute to the development and sustainability of the project, working in a European environment and getting financial support.

The GATEKEEPER project is an EU-funded initiative under the Horizon 2020 Framework Programme. Its main objective is to create a GATEKEEPER that connects healthcare providers, businesses, entrepreneurs, elderly citizens and the communities they live in. This connection between stakeholders will promote an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for older adults.

Relevant information:
Aim: actively engage new technological members in the GATEKEEPER Ecosystem, supplying new Artificial Intelligence (AI) and Big Data applications, tools or components which will be incorporated into the Gatekeeper portfolio and offered to pilots and platform designers and developers.
Target: start-ups, SMEs, Midcaps, Industries and Research technology organisations
Budget: 600,000€, with a maximum of 10 projects funded
Deadline: 29/01/2021
Project duration: 12 months
For more information: https://lnkd.in/eHdFA7z

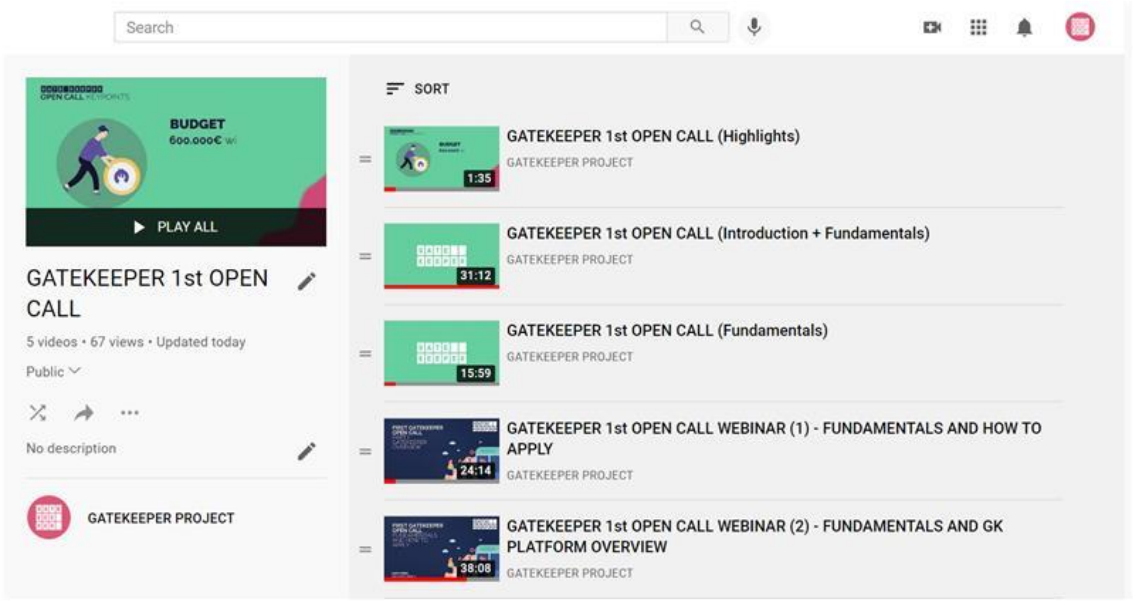
#GKOpenCall #GatekeeperEU #innovation

Figure 10. Example of a post on the GATEKEEPER group

These messages were updated to cover the 5 main phases of the social media campaign. In additional to posting these messages on the LinkedIn group, project partners were also encouraged to post the messages on their own personal LinkedIn profiles.

YouTube

In this channel a specific playlist was created to allocate the two webinars performed regarding the 1st Open Call and the audio-visual materials created. The five materials available regarding accumulates more than 1750 views.



Search

SORT

GATEKEEPER 1st OPEN CALL

5 videos • 67 views • Updated today

Public

No description

GATEKEEPER PROJECT

PLAY ALL

1:35 GATEKEEPER 1st OPEN CALL (Highlights)
GATEKEEPER PROJECT

31:12 GATEKEEPER 1st OPEN CALL (Introduction + Fundamentals)
GATEKEEPER PROJECT

15:59 GATEKEEPER 1st OPEN CALL (Fundamentals)
GATEKEEPER PROJECT

24:14 GATEKEEPER 1st OPEN CALL WEBINAR (1) - FUNDAMENTALS AND HOW TO APPLY
GATEKEEPER PROJECT

38:08 GATEKEEPER 1st OPEN CALL WEBINAR (2) - FUNDAMENTALS AND GK PLATFORM OVERVIEW
GATEKEEPER PROJECT

Figure 11. YouTube play specific play list

2.2.3 Newsletter

The GATEKEEPER database was created from the beginning of the project, gathering valuable contacts from the partners of the consortia and the contact form on the website, with the purpose of sharing with them the achievements and outcomes. In order to feed this database, the OC team searched among the local networks for accelerators and influencers with intention of spreading the word to the main start-ups and SMEs in Europe. Additionally, through the registration process of the OC section, more than 1.000 contacts were gathered, which represents a great result in terms of interest about this funding opportunity.

Considering the wide audiences engaged, regular communications in newsletter format were sent to inform about the points listed below:

- GATEKEEPER news and activities
- Open call Information
- Upcoming events and webinars
- Website articles about the project
- Other activities by partners or hubs of interest to the network
- Community of interest

2.2.4 Webinars

Webinars are a technologic tool that significantly support and maximizes the dissemination of the announcement and progress of the open call. Holding a Webinar gives the opportunity to present the project and its open call extensively while simultaneously allows the interaction with the potential applicants.

Three sessions were performed, and the details are shown in the chapter 8 of this deliverable.

2.3 Publication of the call

The main website of the open call included a section with general information of the call. This section was the first that applicants read and summarized those most important points of the call in a concise way. The following information was provided:

- Dates of publication October 31st, 2020
- Deadline February 28th, 2021
- Start and end dates of the selected projects from June 1st 2021 to May 31st 2022
- Language in which the proposal should be submitted, English
- Email contact address opencall@gatekeeper-project.eu
- Total amount of funding for the call 600k€
- Funding per project 60k€ approx.

Open Call 1 was announced in month 13 (October 2020). The Open Call was disseminated through various social media channels, including Twitter and LinkedIn groups with interests in IoT, and via relevant mailing lists from European projects.

The dissemination was organized and largely executed by Medtronic. In order to streamline the communication efforts of different partners, Medtronic compiled a dissemination toolkit that consisted of a dedicated communication plan, standard texts for tweets and emails, visuals. The dissemination kits were intended to make sure that all partners were supported in their role of reaching out to communities close to them.

The call was intended to be closed on 28th of February 17:00 CET. Late submissions were not accepted.

3 Calendar

The agenda for the first Open call, which it includes below, was published in the main website of the project www.gatekeeper-project.eu

3.1 Agenda first open call

- October 31, 2020: Open call launch
- February 28, 2021: Deadline for applications
- March 31, 2021: Winner publication
- May 2021: Agreement signed
- June 2021 Start deployment

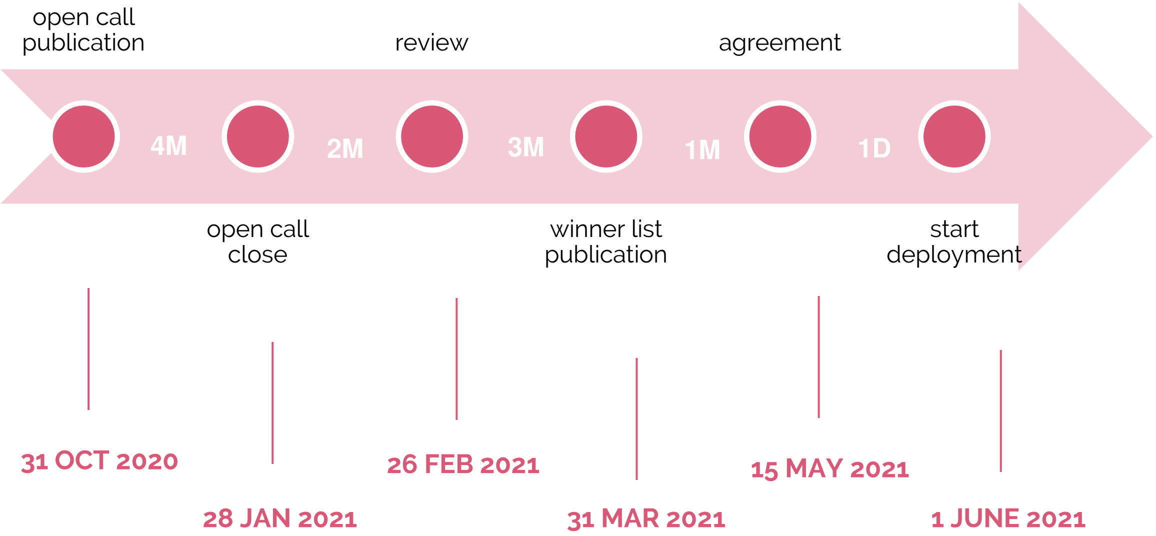


Figure 12. Timeline First Open call

4 Submissions

The proposals were submitted to the email address

https://gatekeeper.submitsquare.com

One hundred and fourteen proposals were received. 1 of the proposals were rejected, because of their duplication with other already submitted, It is not included in the details we give below. We received proposals from 23 different countries all over the world. The following sections show their distributions per country and participant type.

4.1 Submitted proposal by country

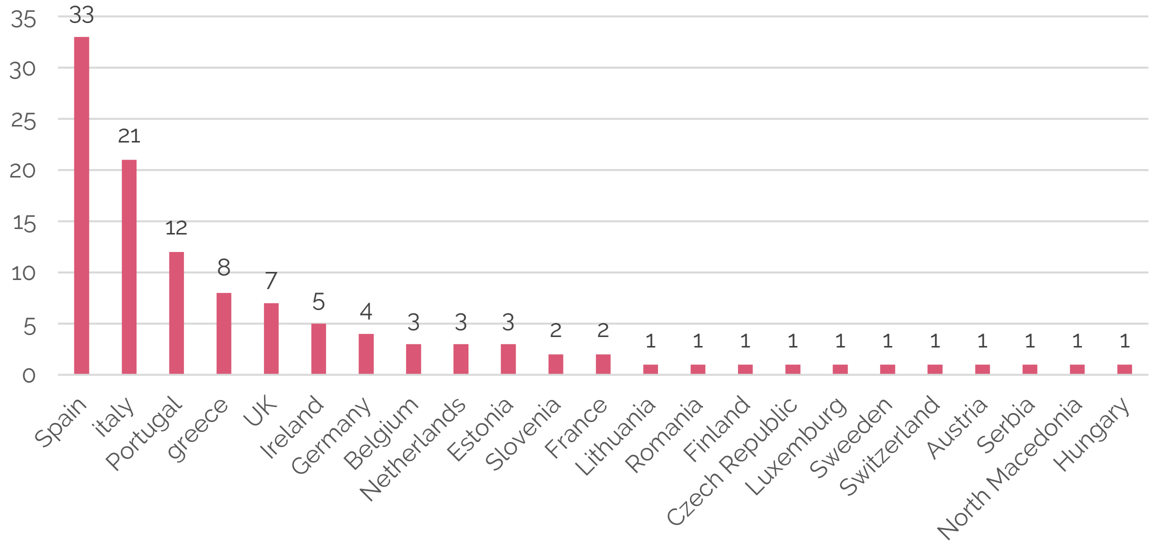


Figure 13. Number of proposals by country

4.2 Submitted participant type

While most of the proposals were submitted by SME's, we also received proposals from universities, technological centres and start up's.

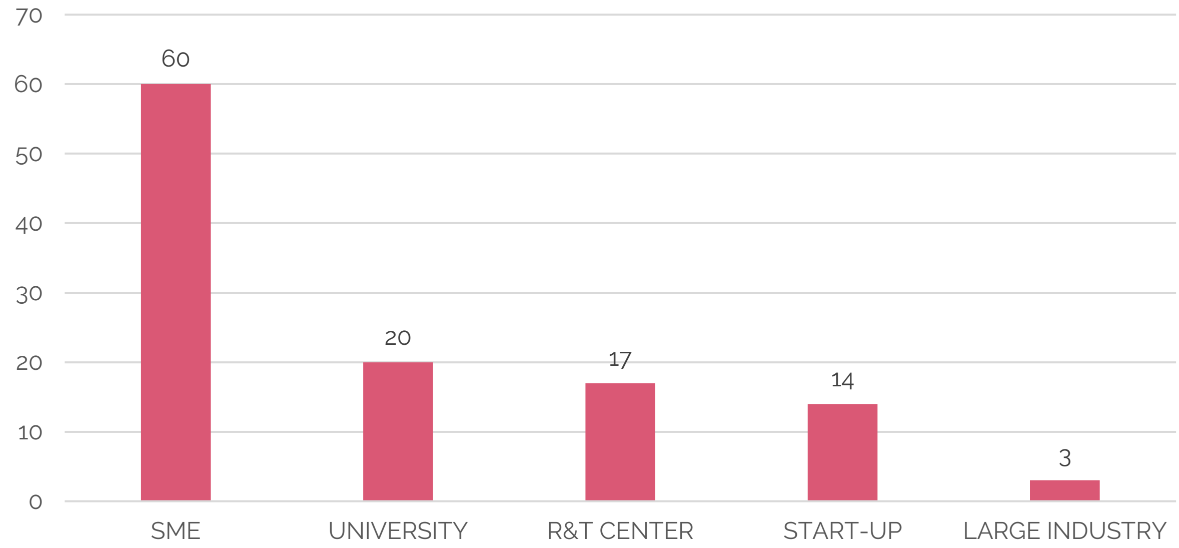


Figure 14. Number of proposals by participant type

4.3 Submitted proposal per challenge

Most of the proposals were applied for the challenge C2, risk detection and timely response, followed by C6 embedded ML in smart devices and C4 Increasing insights from HER's un-structured data.

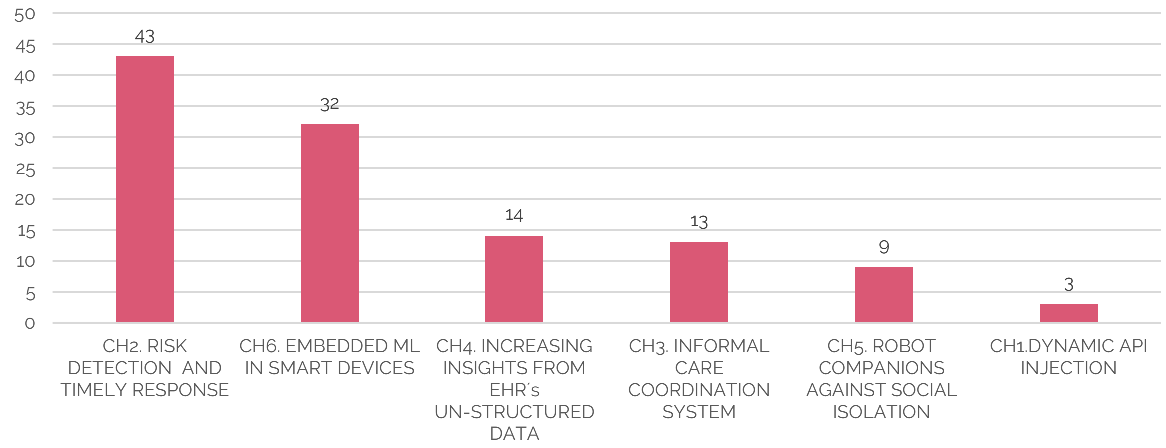


Figure 15. Number of proposals by challenge

Table 1. Challenge description

#	CHALLENGE	DESCRIPTION
1	Dynamic API injection	This challenge is open to proposals providing plugins for Express Gateway for dynamic APIs
2	Risks detection and timely response (mid-term and time critical)	This challenge is open to proposals providing intervention planners for risks and emergency detection
3	Informal care coordination system	This challenge is open to proposal addressing the coordination of informal careers
4	Increasing insights from HER's un-structured data (risks prevention)	This challenge is open to proposals capable to extract meaningful information from EHR´s convertible into actionable insights
5	Robot companions against social isolation	This challenge is open to proposal addressing the design and development of robotic platforms
6	Embedded ML[4] in Smart Devices	This challenge is open to proposal addressing the design and development of innovative prototypes of hardware /software solutions.

[4] ML, Machine learning

5 Evaluation of the proposals

5.1 Evaluation procedure

Every proposal is checked to ensure that it meets requirements before it is sent for evaluation to the Open Call Review Board (OCRB). This board consists of an external and independent group of experts, who will be monitoring the whole process to ensure tracking of every action. Open Call Review Board is composed by external and independent experts in different backgrounds (Clinical aspects, technological knowledge and business).

In this phase the evaluation process used a strategy of double-blind peer review, which means each proposal was reviewed by 2 reviewers and the identity of both experts and proposers is kept confidential from each other. The evaluation is performed remotely, and each expert submits an evaluation report for each proposal s/he evaluates using the evaluation portal, submittable.

The overall maximum score is 25. For a proposal to be considered for being selected for funding, the score has to pass a threshold of 3 out of 5 in each individual category (for the double-weighted impact, this means a score of at least 6 out of 10). The total sum of the individual scores must reach the minimum threshold of 20 points.

If there is misalignment of 3 points or more between both reviewers in each evaluation criteria (that means consensus not reach), a third reviewer will be part of the group to evaluate the proposal in a second round. The idea is to create a common agreement in the final decision. The final list of the funded projects was created according the ranking list of the proposals and assuring a good integration into the platform

Notifications on funding or rejections was sent out by the ending of March 2021.

5.2 Evaluation criteria

Each proposal was evaluated based on the already defined criteria. Reviewers scored and ranked each proposal according to a grid consisting of a quantitative score for each of the following evaluation criteria:

1. **EXCELLENCE:** Soundness of concept, quality of objectives and innovative elements present in the proposal. Max=5. Threshold =3
   - How well does the proposed solution address the challenge as detailed in the open call text?
   - Are the proposed objectives clear and pertinent?
   - Is the concept sound and shows a clear plan for development of a working solution?

2. **IMPLEMENTATION:** quality and efficiency of the implementation and the management. Feasibility of the workplan, quality and effectiveness of the technical methodology, including the workplan, contribution to collaboration with GATEKEEPER to achieve objectives of the project, appropriateness of the allocation and justification of the resources to be committed (staff, equipment…) Max=5 Threshold =3
   - How effectively will be the Application Experiment be managed? Is the proposed work plan coherent and effective?
   - Are deliverables, milestones and deadlines defined and adapted to the goals of the proposals?
   - Is the allocation of tasks and dedicated resources (e.g. human capital, equipment, man hours, etc.) appropriate and necessary to necessary to perform the scope of the proposal and achieve its objectives?
   - Are the costs clearly defined and aligned with the required efforts?
   - Does the third party possess the technical skills and abilities necessary to perform the scope of the proposal?

3. **IMPACT AND SUSTAINABILITY**: Potential impact through the development, dissemination and use of project results, in which way the proposal contributes to further maturity, integration and interoperability of gatekeeper AI solutions, and explain if you consider any further support after your participation in GATEKEEPER project. Max=5 Threshold =3
   - Does the proposal enhance innovation capacity and the integration of new knowledge?
   - Assessment of resources required to demonstrate you have taken into account all key elements for the success of your project to reach exploitation.
   - Strategic fit for the company explaining why this project is important for your company.

The selected proposals were reported to the gatekeeper project officer of the European Commission for a final granting decision

5.3 Evaluation form

The reviewers had access to the evaluation portal to enter scores and comments for each proposal they evaluate. The evaluation form below is included here to help reviewers prepare well in advance before they enter the scores via online portal.

The overall maximum score is 25. For a proposal to be considered for being selected for funding, the score has to pass a threshold of 3 out of 5 in each individual evaluation criteria.

Each evaluation criteria was articulated in different categories which will be scored from 0 to 5 points.

The individual scores have the following interpretation:

0 - Fail: The proposal fails to address the criterion under examination or cannot be judged due to missing or incomplete information.

1 - Poor: The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.

2 - Fair: While the proposal broadly addresses the criterion, there are significant weaknesses.

3 - Good: The proposal addresses the criterion well, although improvements would be necessary.

4 - Very good: The proposal addresses the criterion very well, although certain improvements are still possible.

5 – Excellent. Proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

6 Selected proposals

Eleven proposals were selected, which we show below in the following tables, together with a brief description of the proposal, the country and the institution or company they came from, the amount of money they received.

Table 2. Envira

Proposal name	
Proposal short name	ENVIRA
Proposal description	Nanoenvi IAQ is a commercial solution for environmental monitoring at indoor locations. Nanoenvi IAQ system is composed by sensor devices to be deployed and a federation platform of services from Envira, but also from other third-party partners, providing analytics and tools for data exploitation. Interoperability within this ecosystem is achieved by applying WoT open standards (each device and service is managed "as a Thing") One of the most demanded features are the "Environmental Indices Calculation Services", which are AI services to calculate relevant standard environmental indices for industries and people such as: air quality index, thermal comfort index, COVID19 transmission risk index, environmental safety for asthmatic people at work locations index, etc. The objective of the present proposal is to integrate Nanoenvi IAQ environmental indices into GK ecosystem.
Country	Spain
Institution/Company	Envira Sostenible S.A.
Amount	60.000 €

Table 3. Spirocco

Proposal name	
Proposal short name	Kanban based organizer for informal care
Proposal description	Our development is a Kanban-based care organizer mobile application relying on the GATEKEEPER ecosystem. The app can be used to schedule and reschedule tasks, organize and monitor suggestions and needs generated by the elders, informal and professional careers in an intuitive way, making it easy to use for elderly people. With the help of Kanban cards, it logs and organizes tasks, and makes the current and historical data, and the schedule available to professionals, informal careers, family members and others involved in carrying. Text and video chat for bidirectional communication, as well as emergency call functions are also included in the app. Different medical and home monitoring devices can be integrated into the system, the data of which are also stored on the server and made available to professionals via the web interface. An AI-based machine learning algorithm is used to evaluate the historical data for early-detection and prediction of interventions, additional needs and tasks, as well as load estimation and bottlenecks of local informal caregiving ecosystems.
Country	Hungary
Institution/Company	Spirocco Kft
Amount	59.718,75€

Table 4. Braingaze

Proposal name	
Proposal short name	Bgaze
Proposal description	Cognitive disorders, specifically dementia and Alzheimer's disease (the most common subtype), are one of the leading causes of ill-health and disability globally, with high level of social and economic burden. Efforts to diagnose dementia and Alzheimer's disease (AD) at earlier stages are being doing as a means to maximise treatment options, adapt healthier lifestyles and enable patients to 'prepare for their future'. People affected by dementia also present visual and ocular movements problems, which include decreased visual acuity, poor colour discrimination, and visual field loss. Our studies show a gradual change in a novel type of minuscule, involuntary eye movement that is triggered when we attend and memorize objects as the neurodegenerative process progresses. This marker is termed Cognitive Vergence. BRAINGAZE assesses Cognitive Vergence through in-house developed sensory tasks and relates them with the cognitive level in order to diagnose impairments. Our game-changing innovation, BGaze system, is a diagnostic software based platform that make use of Cognitive Vergence biomarker. Cognitive Vergence has proven to be intimately linked to cognitive brain processes. Through scientific proven attention tasks performed by patients at the clinic or at home together with AI-based classification algorithms and deep/machine learning techniques, BGaze allows clinicians to objectively monitor cognitive health and detect people at risk developing dementia within minutes with a 93% diagnostic accuracy and up to ten years before the first clinical symptoms of dementia appear. Thus, it can be used as a non-invasive, robust biomarker to assess cognitive status on a regular basis in elderly. The solution addresses the challenges of the Lifestyle-relate early detection and interventions call.
Country	Spain
Institution/Company	Braingaze
Amount	44.537,50 €

Table 5. Ab.Acus

Proposal name	
Proposal short name	SPEAKapp - Remote speech assessment for therapy follow up and morbidity monitoring
Proposal description	Speech and language assessment is a powerful yet unobtrusive tool that can support clinical diagnosis and monitoring in a wide range of clinical conditions implicating cognitive and affective symptoms such as Diabetes, Stroke, and Parkinson's disease. Recent advances in Natural Language Processing (NLP) have proven their ability to both overcome the practical barriers of data acquisition and analysis, as well as to yield reliable digital endpoints of cognitive and affective status. However, in order to effectively build upon these potentialities and hence meet real clinical and research needs, it is pivotal to bridge the gap between end users and clinicians on one hand, and developers and researchers on the other hand. SPEAKapp is a functional app prototype for mobile devices to deliver and analyse speech and language data, specifically developed for clinical and research purposes. Based on cutting-edge AI technologies for the analysis of audio waves and semantic contents of speech outputs and incorporating standard assessment tools, SPEAKapp specifically address the GATEKEEPER's Challenge 6 Embedded Machine Learning in Smart Devices. SPEAKapp is an easy-to-use yet powerful tool that put the end user at the centre of the clinical process, support and empowering both patients and clinicians in the everyday management and monitoring of the disease. SPEAKapp will be made available to GATEKEEPER's Pilot Sites through the GATEKEEPER platform, thus enabling its evaluation and benchmark assessment through access to technology, test beds and data sets
Country	Italy
Institution/ Company	Ab.Acus srl
Amount	59.937,50 €

Table 6. Nissatech

Proposal name	
Proposal short name	Personal Health Twin for ensuring healthier independent lives for senior people
Proposal description	A full adoption of smartwatch technology for personalized medicine is lacking a more intelligent and personalized processing of the collected data, on the smartwatch itself. This would lead to the smart personalized healthcare ensuring healthier independent lives for senior people, which is the ultimate goal of this proposal (and also one of main objectives of the GATEKEEPER project). In the nutshell of the proposal is the complex modelling of a person health-related behavior using advanced AI and big data techniques. The main goal is to create digital replicas which will enable a comprehensive analysis of the health of a person, so called Personal Health Twin. In this way we create a holistic, multi model view on the behavior of a person, which can be used for the creation of various services for remote monitoring, early detection and intervention. Due to resource-constrained nature of the smartwatch, this process should be performed in a very efficient way which is one of the unique selling points in this proposal, based on our huge experience in developing smartwatch based commercial solutions (apps and backend). Indeed, this proposal will leverage the already existing system for smartwatch-based personalized fitness (Smart4Fit, TRL9), by extending the personal and intelligent processing on smartwatch for healthcare scenarios and extending the personal model based on GATEKEEPER Information model. The proposal addresses the Challenge 6 “Embedded ML in Smart devices”, planning the implementation of three services, which cover three main aspects of the Personal Health Twin: a) advanced medium-long term behavioural changes detection based on activity detection, b) mental condition monitoring and c) remote health status monitoring, early detection and intervention. Regarding large scale pilots, the goal is to enlarge and extend selected ones (starting with Basque country, Saxony) with planned services, available in the GATEKEEPER's platform. The proposal is very aligned with our business strategy and opens huge market opportunities in the smart personalized

	healthcare domain.
Country	Serbia
Institution/ Company	Nissatech
Amount	59.955€

Table 7. Gripwise

Proposal name	
Proposal short name	Fragile - FasteR and AGILE way to assess frailty status in network.
Proposal description	Informal care has a key communicative role in helping physicians to learn about the patient and in facilitating information exchange between the doctor and the patient. Nowadays 60% of the elder population of Europe suffers from some level of physical frailty, with the estimated costs to EU Healthcare Systems surpassing 81 Billion €/year. Frailty is the most problematic sign of the aging population and a strong indicator of physical vulnerability. It can be assessed using 5 criteria, which rank the elderly as normal, pre-frail or frail. Based on this, frailty screening, diagnosis and treatment are of major relevance, more so, because Frailty is potentially modifiable with adequate and opportune simple interventions. To address this situation and assess Frailty in the elderly, we created Gripwise, a technology based on a smart load cell, with an accelerometer and gyroscope, all integrated and connected into a system capable of a full frailty workflow assessment, done in a simple and fast way. Its streamlined workflow, with basic training, allows caregivers to assess Frailty even without technical skills. The app integrates all results and provides a full report which is transferred to a Cloud platform, allowing diagnosis of the elderly by health professionals. This solution squarely meets GATEKEEPER challenge #3. With Gripwise, caregivers can help to detect Frailty early and share results with the Health Care Systems. This solution allows health professionals to diagnose and follow-up on their patients even at a distance. This addresses the issue of sharing the responsibility of caring between the caregiver and the physician, prescribing personalized physical activity and nutrition to help maintain energy, functionality, and quality of life of the elderly. This bi-lateral communication can reduce the frequency of doctor's appointments and support routine activities, causing a reduction in overall health costs, while still maintaining quality of life.
Country	Portugal
Institution/ Company	Gripwise Tech, Lda
Amount	42.000€

Table 8. PROMPTLY

Proposal name	
Proposal short name	AI4DM
Proposal description	The AI4DM addresses the GATEKEEPER scope of delivering an advanced digital solution for personalized early detection and intervention, improving the quality of life of patients, while providing significant efficiency gains to health care services. This is achieved by offering AI predictive modelling services that, by assessing the condition of older adults suffering from diabetes type 2, and under a time sensitive intervention and operational plan, will detect risks from short (hypoglycaemias) to mid-long term (diabetes comorbidities). This will provide the possibility of issuing alarms that may trigger a needed intervention, balanced with the probability of the risk occurring
Country	Portugal
Institution/Company	Promptly Health
Amount	59.981,25€

Table 9. University of Vigo

Proposal name	
Proposal short name	Panoramix: Serious Games for the Early Detection of Cognitive Impairment
Proposal description	This proposal aims to incorporate in the GATEKEEPER platform a battery of serious games to detect cognitive impairment in elder adults. This game battery assesses different cognitive areas and uses machine learning techniques to discriminate among players suffering from mild cognitive impairment or Alzheimer disease from healthy adults. Using the battery, it is also possible to identify individuals likely to develop cognitive decline, to predict the future evolution of cognitive decline and to contribute to keep the cognitive reserve of elder adults. The battery complies with the psychometric properties set of the Standards for Educational and Psychological Testing, that is, it meets all the clinical criteria to be considered as a valid screening tool.
Country	Spain
Institution/Company	University of Vigo
Amount	59.625€

Table 10. CognitEye

Proposal name	
Proposal short name	On-device video semantic concept recognition: a wearable personal vision assistant
Proposal description	Imagine a day when the 30 million blind and visually impaired Europeans can use their cell phone with the CognitEye app to describe to them the surrounding environment automatically by recognizing the semantic concept of the captured video. The video is continuously captured via a camera embedded in a wearable device and users hear the description of the scene, objects, and activities through the bone conduction headphones. All this information is provided while fully preserving privacy as the information does not need to leave the device. The current vision assistant systems such as Seeing AI from Microsoft or TapTapSee run on cloud-based Graphical Processing Units (GPUs) servers because video recognition typically requires an enormous amount of processing power. The major drawback is that users have to transfer their personal data to the cloud using a high-speed Internet connection. CognitEye is working on an important breakthrough and offers a completely game-changing technology: the CognitEye software makes on-device video analysis possible. It can extract the semantic interpretations from the captured video and describe the scene for the visually impaired users. The CognitEye software relies on the Neural Processing Unit (NPU) which is built into the mobile processor to utilize advanced deep neural networks and provide new levels of vision intelligence. The aim of this proposal is highly in line with the GATEKEEPER challenge on embedded ML in smart devices (Challenge#6). To this end, we get technical supports from the parent company SensifAI. They publicly launched the world's first real-time video recognition mobile application embedded in NPU flagship smartphones. The SensifAI mobile beta app is already available online on Google app store for free.
Country	Belgium
Institution/Company	CognitEye
Amount	43.750€

Table 11. Quadible Ltd

Proposal name	
Proposal short name	MENTAL: Secure mental condition and behaviour change detection for elderly people
Proposal description	The world's population is ageing across every country and continent. According to the World Economic Forum, "never before have such large numbers of people reached the older ages (conventionally defined as ages 65 and up)". New form of medication, vaccines as well as better way of life has led to the increase of the age of the population. In the meantime, elderly people require a larger amount of support from the community and healthcare. This creating large pressure to the national healthcare systems considering that the majority of the actions require healthcare personnel involvement or even 24/7 observation for assistance or daily behaviour monitoring to detect behaviour changes as well as mental conditions. This creates huge amounts of personnel costs, lack of healthcare staff, the potential for human error as the monitoring process is fully human-based and does not allow elderly people to live an independent life in their homes. MENTAL project focuses on improving the detection and prevention of behaviour changes and mental conditions for elderly people, to reduce productivity costs for healthcare organisations, allow them live independently at their homes, while improving the security/privacy and trustworthiness of healthcare solutions. MENTAL will integrate and deploy an AI-based behaviour analysis solution at the GATEKEEPER framework to fully automate the behaviour monitoring process allowing the derivation of fine-grained behavioural information. A 2-week pre-pilot will be performed at the beginning of the project to validate the correctness of the integration. Following, a 10-month pilot will validate the interoperability, scalability and user satisfaction of the MENTAL platform and the GATEKEEPER platform at four pilot sites. Information related to the user experience, service quality etc. will be monitored during the pilots, to measure the success of the project. Dissemination and communication activities will maximise the international outreach of the GATEKEEPER project at a worldwide scale.
Country	UK
Institution/ Company	Quadible
Amount	59.998,75€

Table 12. NIM Competence Center for Digital Healthcare GmbH

Proposal name	
Proposal short name	Radiolytx DOPA
Proposal description	An AI Module for the early diagnosis of PD using EHR unstructured data. In this project we address the GATEKEEPER challenge of increasing insights from Electronic Health Records (EHRs) unstructured data in order to identify novel clinical paths for the risk of PD in the challenging case of subclinical patients.
Country	Germany
Institution/Company	NIM Competence Center for Digital Healthcare GmbH
Amount	37.625€

7 Management and administrative organizations

As a part of the contract, newly joined third parties receive an obligation to track progress to the related beneficiaries and take part in demonstrations. In addition to periodic progress reports they will be instructed on GATEKEEPER progress tracking tool currently in use by all beneficiaries.

The GATEKEEPER mentor assigned to each first open caller is in charge to supervise the entire management of the projects to help and control the progress of the development and implementation of the project.

Any breach in the execution of the activity under contract will be processed within GATEKEEPER consortium, and the relative costs will be considerate ineligible.

To manage the Open Call 1 execution and assure that everything is going to proceed as planned and reach the goals of all the parties, in WP2 GATEKEEPER partners created a "follow-up process" to detail the procedure in place for the management and administrative organization of the projects and partners.

7.1 Follow up process

The "follow-up" process was designed and put in place to define the procedure for the open calls follow-up.

The main objectives of this process are:

- To integrate Open Calls in GATEKEEPER Ecosystem
- Establish a constant and fixed connection point between GATEKEEPER partners and open callers
- Facilitate partners coaching and communication.
- Ensure that open callers' solutions are implemented and deployed.
- Review periodically the status of the projects

At the same time one specific person from WP5 has been assigned as an internal "mentor" to each Open Call project as supervisor.

Table 13. Management Distribution WP5 per OC

Project	Mentor assigned	Partner
Envira	Paolo Zampognaro	Engineering
Spirocco Ltd.	Alessio Antonini	The Open University (OU)
Braingaze	Leire Bastida	Fundacion Tecnalia Research & Innovation (tecnalia)
Ab.Acus	chronaki@hl7europe.org	HL7 Foundation
Nissatech	Salman Haleem	University of Warwick
Gripwise	Eleni Georga	Panepistimio Ioanninon (UoI)
Promptly	Sergio Copelli	MultiMed Engineers srls (MME)
University of Vigo	David Martin Barrios	Ibermatica
CognitEye	David Ragget	GEIE ERCIM EEIG – W3C/ERCIM (W3C)
Quadible Ltd	Bangfu Tao	Samsung
NIM Competence Center	Claudio Caimi	Hewlett Packard Italiana srl (HPE)

2.2.1 Monthly meeting

To have a better and direct management and administrative organization of the OC projects the followers have specific monthly meeting with open call partners.

The main characteristics of the monthly meetings focus on:

- One meeting per month per "open caller"
- The meetings are done usually via teleconference
- The meetings serve as official overview of the status of the projects

The objectives are:

- Monitor the progress of the project
- Check tasks and deliverables status
- Facilitate partners communications
- Collect information and activities status reports
- Evaluate possible risks, issues or eventual delays and be able to react in time to find solutions.

Responsible: WP5 OC mentors

2.2.2 Review Process

Mid-term and final review meeting:

- Review meetings characteristics:
    - One Face2Face or online review meeting at half of the project
    - One final Face2Face or online review meeting at the end of the project
    - The meetings are done in the same day at a prearranged and fixed location and time per all open callers.
    - Representatives from each OC partner need to be present
    - Representatives of GATEKEEPER partners supervise the review process
- Objectives:
    - Have a presentation and demonstration of each open call project
    - Look for evidences of the progress (verification)
    - Collect all the reports and documentation related to the development and implementation of the projects
    - Discuss the outcome of periodic reports
    - Evaluate the status and in case provide review on possible issues.

Responsible: WP7 + Coordination

2.2.2 Standard reporting

For facilitating the collection of standard and critical information for each open call project we framed a specific report template called "GATEKEEPER Status Form" (See copy in Appendix J) which is meant to be completed by open callers to report their progress.

- It needs to be filled every month for monthly reports and extended version for review

These status reports are used to provide information regarding:

- Status of performed activities (work plan, deliverable)
- Integration in the platform
- Dissemination and communication activities (external and internal
- Hot topics

7.2 Relationship with other WP

Moreover, in addition to the integration of projects in GATEKEEPER we had to manage the implication related to the inclusion of open callers in the GATEKEEPER ecosystems, market and integration in working packages activities.

From the technical developments, the use-cases deployments and extensions, new users base and additional data we established flows of information and interactions between GATEKEEPER Working Packages and OC Partners, e.g.:

- WP5 for the technical integration related to GATEKEEPER
- WP9 Socio-economic impact assessment and evaluation
- WP2 Deployment sites definition, execution and coordination
- WP3 for the integration within the offering Portfolio of GATEKEEPER Catalogue
- Contributions to deliverables
- Contributions to reports, assessments

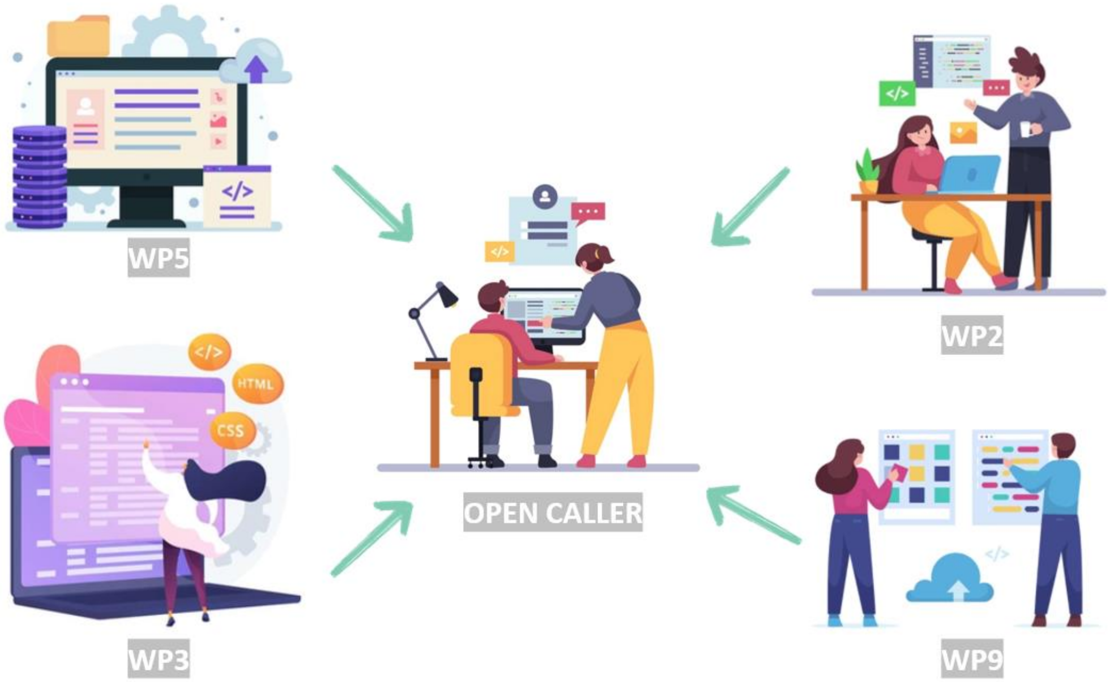


Figure 16. interactions between OC and GK WP

8 Technical support

The present section includes information of the technical support that has been provided to open callers. First of all, the main technical support is provided by mentorship (already described in section 7.1) furthermore there are also other channels that are designed for technical support to developers:

- GATEKEEPER developer portal
- GATEKEEPER Slack channel
- Mailing support
- Technical webinars.

8.1 GATEKEEPER developer portal

GATEKEEPER is creating a complex ecosystem that includes an owned cloud environment as well as several software components that interact with each other.

One component developer within the project that provides technical support for open callers and in general every developer is the developer portal.

The GATEKEEPER developer portal is the interface between the set of APIs, SDKs, or other interactive digital tools and the Thing Description of the GATEKEEPER components. The portal can play several roles to achieve the provisioning of the technical support, GATEKEEPER developer teams publish their Thing Description component that are translated into "Swagger/Open API Spec" (or RAML, API Blueprint, I/O Docs, WSDL, etc) documentation within the developer portal.

However, reference documentation (WoT and OpenAPI spec) is only one part of the GATEKEEPER developer portal. It not only contains API or SDK reference documentation, but it is also a place where developers can learn from the material that developer have uploaded in regard to their components.

Within the GATEKEEPER developer portal there is the learning section that collect all the public learning material, including tutorials, examples, getting started guides, etc., that every contributor of the GATEKEEPER platform have created.

This learning materials are grouped by topic and are available within the GATEKEEPER developer portal. Further details about the GATEKEEPER developer portal are available in the D5.1.2.

8.2 GATEKEEPER Slack Channel

Slack[5] is a workplace communication tool, that means a multiplatform app (web, mobile and desktop) that provides a single place for messaging, tools and files. This means Slack is an instant messaging system with lots of add-ins for other workplace tools. The add-ins aren't necessary to use Slack, though, because the main functionality is all about talking to other people. There are two methods of chat in Slack: channels (group chat), and direct message or DM (person-to-person chat).

Channels in Slack can be public, meaning any member can see and join that channel, or private, meaning only members of that channel can see it or invite others to join. DMs are always private, although they can include up to 8 people.

The chat window is where all the actual communication happens. You can read any reply to messages, use emoji reactions, add gifs, see RSS feeds, set reminders, get add-in notifications, and various other bells and whistles. But more than anything, this is where you talk to people.

Within GATEKEEPER we are using a Slack channel for developer where group chats are connected to specific Gatekeeper components such as GATEKEEPER infrastructure, Data Federation, Thing Management system, etc..

In this context an open caller developer can reach directly the component owner and share at same time the issue that he has detected.

8.3 Mailing support

Traditional support channels, such as email support, are also available for open caller.

The mail support is organized in a hierarchical way with the open call mentor as the delivery points between the open caller technical request and the GATEKEEPER platform component owners.

Following the open caller actor map (Figure 7), the open caller requests are sent to the most relevant actor within the GATEKEEPER ecosystem.

[5] Slack, https://slack.com/intl/en-it/ , last access September 2021

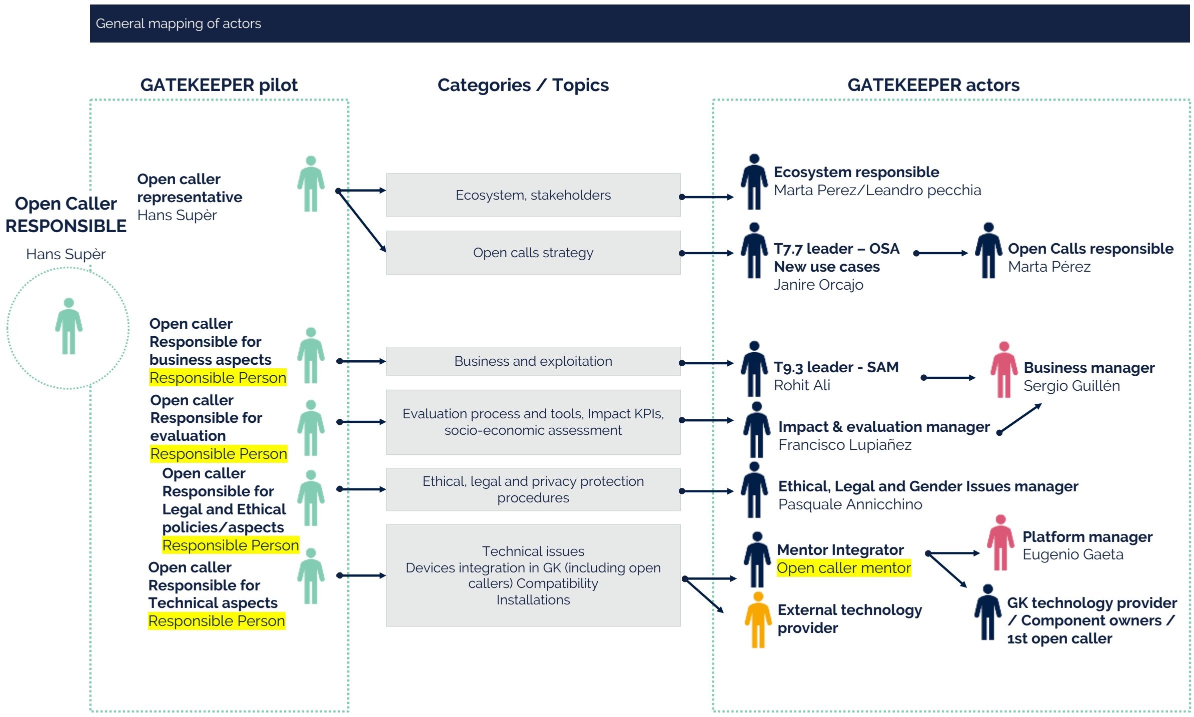

General mapping of actors
GATEKEEPER pilot
Categories / Topics
GATEKEEPER actors
Open Caller RESPONSIBLE
Hans Supèr
Open caller representative
Hans Supèr
Open caller Responsible for business aspects
Responsible Person
Open caller Responsible for evaluation
Responsible Person
Open caller Responsible for Legal and Ethical policies/aspects
Responsible Person
Open caller Responsible for Technical aspects
Responsible Person
Ecosystem, stakeholders
Open calls strategy
Business and exploitation
Evaluation process and tools, Impact KPIs, socio-economic assessment
Ethical, legal and privacy protection procedures
Technical issues
Devices integration in GK (including open callers) Compatibility
Installations
Ecosystem responsible
Marta Perez/Leandro pecchia
T7.7 leader – OSA
New use cases
Janire Orcajo
Open Calls responsible
Marta Pérez
T9.3 leader - SAM
Rohit Ali
Business manager
Sergio Guillén
Impact & evaluation manager
Francisco Lupiañez
Ethical, Legal and Gender Issues manager
Pasquale Annicchino
Mentor Integrator
Open caller mentor
Platform manager
Eugenio Gaeta
External technology provider
GK technology provider / Component owners / 1st open caller

Figure 17. Open caller actor map

8.4 Technical webinars

Within GATEKEEPER project we have been provided a lot of webinars including technical ones. The GATEKEEPER technical webinar are available for all open callers within the GATEKEEPER Alfresco repository as well as the private space of the GATEKEEPER project web page, the public technical webinars are also linked as learning material in the GATEKEEPER developer portal.

9 Webinar sessions

Webinars are a technologic tool that significantly support and maximizes the dissemination of the announcement of the open call. Holding a Webinar gives the opportunity to present the project and its open call extensively while simultaneously allows the interaction with the potential applicants. This provides a better understanding of the project and what the project is looking for by means of the open call. Moreover, a webinar offers an excellent opportunity to interact with the applicants allowing to clear up any concerns someone may have about the call. The webinars were recorded and placed in the call materials section of the open call to be visualized by anyone interested.

Hold webinars for open call were:

- 1 webinar about The GATEKEEPER Fundamentals: Project, benefits, the open call, eligibility criteria, expectations. Also the application process and how to use the open call platform.
- 2 webinars about the GATEKEEPER Fundamentals and gatekeeper platform overview: The GATEKEEPER Project, benefits, the open call, eligibility criteria, expectations. Also the overview of the GATEKEEPER platform
- 1 webinar exclusive for the reviewers, to explain the project, the submission platform and evaluation aspects.

As mentioned, these four webinars were planned in different moments of the open call

- 25 November 2020
- 16 December 2020
- 3 February 2021
- 3 March 2021

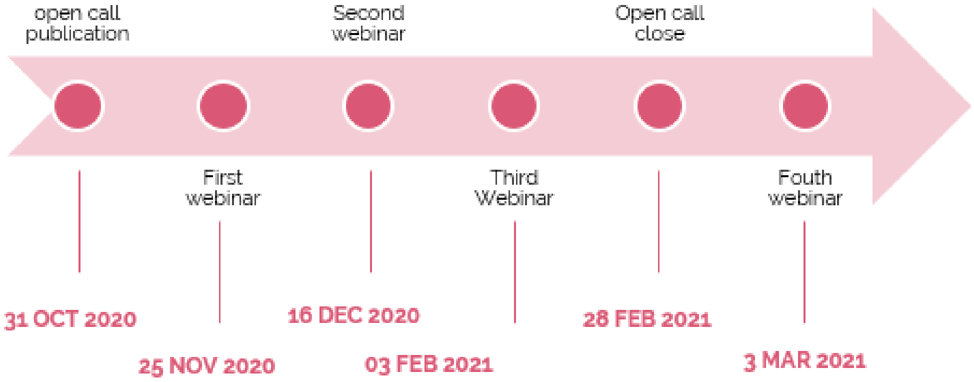


Figure 18. Timeline webinar

10 Financial report

The total budget reserved for the GATEKEEPER Open Calls amounts to EUR 1.200.000€ to be assigned in equal proportions to the two Open Calls. Thus, the total budget for the first open call was € 600,000, which provided OC1 with a capacity of funding 11 projects, each not exceeding € 60,000 in accordance with the EU legislation.

The actual funding and payment status for the 11 winning proposals can be summarized the following way:

Table 14. Funding and Payment Open Call

Winner	Contract amount	Pre-financing 20%	Mid-term payment 50%	Final payment 30%
ENVIRA Sostenible S.A	€ 60,000.00	€ 12,000.00	€ 30,000.00	€ 18,000.00
Spirocco Ltd.	€ 59,718.75	€ 11,943.75	€ 29,859.38	€ 17,915.63
BRAINGAZE	€ 44,537.50	€ 8,907.50	€ 22,268.75	€ 13,361.25
Ab.Acus slr	€ 59,937.50	€ 11,987.50	€ 29,968.75	€ 17,981.25
Nissatech	€ 59,955.00	€ 11,991.00	€ 29,977.50	€ 17,986.50
Gripwise Tech, Lda.	€ 42,000.00	€ 8,400.00	€ 21,000.00	€ 12,600.00
Promptly Health	€ 59,981.25	€ 11,996.25	€ 29,990.63	€ 17,994.38
University of Vigo	€ 59,625.00	€ 11,925.00	€ 29,812.50	€ 17,887.50
CognitEye	€ 43,750.00	€ 8,750.00	€ 21,875.00	€ 13,125.00
Quadible Ltd	€ 59,998.75	€ 11,999.75	€ 29,999.38	€ 17,999.63
NIM Competence Center for Digital Healthcare GmbH	€ 37,625.00	€ 7,525.00	€ 18,812.50	€ 11,287.50
Total	€ 542,591.25	€ 108,518.25	€ 271,295.63	€ 162,777.38
	Reserved budget ↑	Already paid ↑	Open payments ↑	

In addition to payments for funding the winners of the open calls, the other direct costs for the management of open calls include the following items:

1. Contract with submitsquare.com for managing the platform for submission and evaluation process with a total costs of 12,000 € covering the first open call.
2. The submitted proposals had to be reviewed and evaluated by independent experts. Based on the experience from former projects, the contract with the experts foresaw € 200 cost per review submitted. The following table summarizes the list of performed reviews and the related costs:

Reviewer	# of Reviews	Resulted payment	
A.P	9	€	1,800.00
S.P.	8	€	1,600.00
D.H.	11	€	2,200.00
C.N.	10	€	2,000.00
C.L.	5	€	1,000.00
O.C.	7	€	1,400.00
D.C.	10	€	2,000.00
J.V.	5	€	1,000.00
J.H.	10	€	2,000.00
R.R.	11	€	2,200.00
J.M.H.	8	€	1,600.00
N.G.	12	€	2,400.00
A.G.	10	€	2,000.00
J.P.	10	€	2,000.00
S.M.	9	€	1,800.00
V.R.	10	€	2,000.00
C.T.	10	€	2,000.00
E.M.	8	€	1,600.00
C.P.	10	€	2,000.00
S.B.	6	€	1,200.00
H.V.	8	€	1,600.00
A.V.B.	12	€	2,400.00
D.I.	12	€	2,400.00
J.G.	11	€	2,200.00
E.I.	13	€	2,600.00
V.B.	10	€	2,000.00
Total	**245**	**€**	**41,400.00**

Therefore, the sum of all direct costs of the first open call is: € 542,591.25 + € 41400 + € 12000 = 595,991.25€.

11 Conclusion a future work

This document presented the result for the First Open Call performed during year 2021

This deliverable presented the dissemination plan, the calendar of each event performed during the period of the call and the eligibility criteria to be selected as candidate. This deliverable presented the systematic process of running the GATEKEEPER Open Call, Using the knowledge from existing projects and guide provided by the Commission, also the required information to prepare a set of documents that contain general Open Call information

In this deliverable is also presented the evaluation and selection results and the management and technical support to the Open Callers

GATEKEEPER open call received nearly 114 proposals from all over Europe that were evaluated by a team of independent external evaluators. Taking into account the excellence of the submitted proposals as well as the requested funding, GATEKEEPER was able to select 11 proposal for funding instead of the initial 10 due to the high quality of the proposals received. A first description of the solution is already available on this deliverable and will be added in the GATEKEEPER technology inventory.

12 References

European Commission, (2016) support programme operations. Guidance note on financial support to third parties under H2020

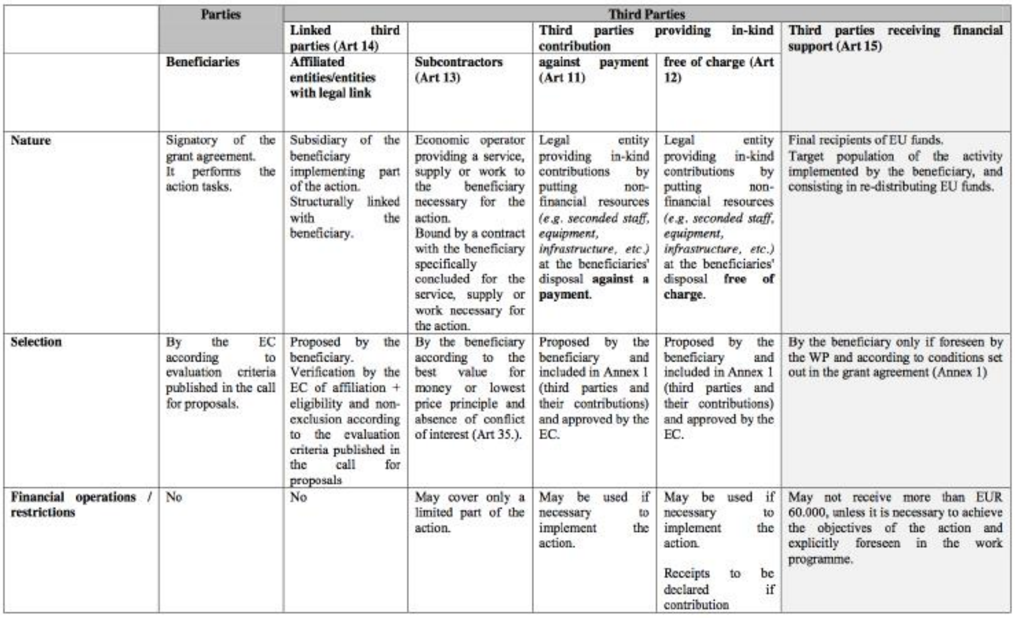
Gallego A., Gaeta E., Belmar A,,Buhid E., Laurin S., Munther M.(2021). GATEKEEPER Project D5.1 Programming Interfaces for Dynamic Services Integration

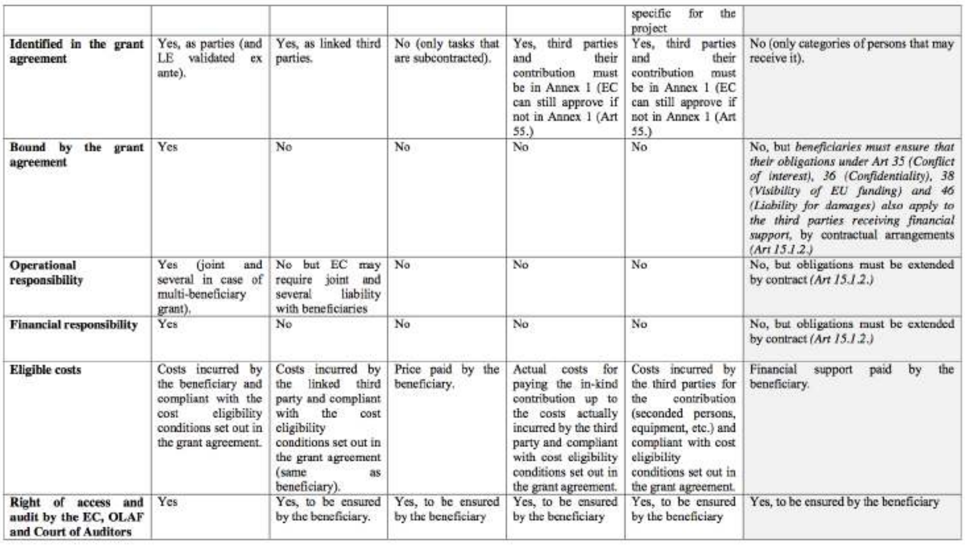
Perez, M., Guillen S., Dantas C., Mackiewicz K., Tageo V. (2020). GATEKEEPER Project D2.1 Initial Ecosystem Management Plan

Perez M., (2020) Gatekeeper project. D2.6 Open call report. Guide for applicant

Appendix A EU guide and templates

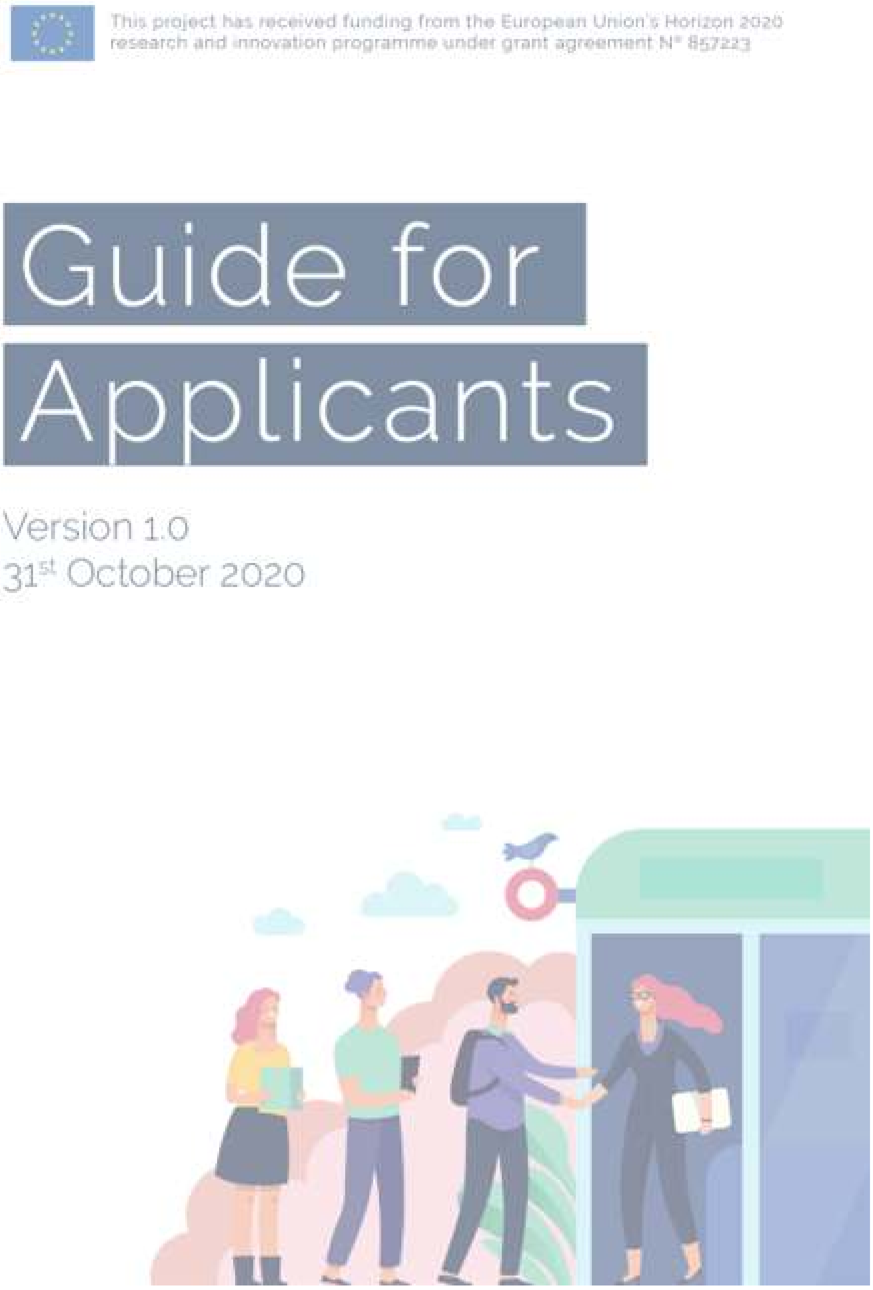
A.1 GUIDANCE OF FINANCIAL SUPPORT TO THIRD PARTIES





	Parties	Third Parties				
		Linked third parties (Art 14)		**Third parties providing in-kind contribution**		**Third parties receiving financial support (Art 15)**
	Beneficiaries	**Affiliated entities/entities with legal link**	**Subcontractors (Art 13)**	**against payment (Art 11)**	**free of charge (Art 12)**	
Nature	Signatory of the grant agreement. It performs the action tasks.	Subsidiary of the beneficiary implementing part of the action. Structurally linked with the beneficiary.	Economic operator providing a service, supply or work to the beneficiary necessary for the action. Bound by a contract with the beneficiary specifically concluded for the service, supply or work necessary for the action.	Legal entity providing in-kind contributions by putting non-financial resources *(e.g. seconded staff, equipment, infrastructure, etc.)* at the beneficiaries' disposal **against a payment**.	Legal entity providing in-kind contributions by putting non-financial resources *(e.g. seconded staff, equipment, infrastructure, etc.)* at the beneficiaries' disposal **free of charge**.	Final recipients of EU funds. Target population of the activity implemented by the beneficiary, and consisting in re-distributing EU funds.
Selection	By the EC according to evaluation criteria published in the call for proposals.	Proposed by the beneficiary. Verification by the EC of affiliation + eligibility and non-exclusion according to the evaluation criteria published in the call for proposals	By the beneficiary according to the best value for money or lowest price principle and absence of conflict of interest (Art 35.).	Proposed by the beneficiary and included in Annex 1 (third parties and their contributions) and approved by the EC.	Proposed by the beneficiary and included in Annex 1 (third parties and their contributions) and approved by the EC.	By the beneficiary only if foreseen by the WP and according to conditions set out in the grant agreement (Annex 1)
Financial operations / restrictions	No	No	May cover only a limited part of the action.	May be used if necessary to implement the action.	May be used if necessary to implement the action. Receipts to be declared if contribution specific for the project	May not receive more than EUR 60.000, unless it is necessary to achieve the objectives of the action and explicitly foreseen in the work programme.
Identified in the grant agreement	Yes, as parties (and LE validated ex ante).	Yes, as linked third parties.	No (only tasks that are subcontracted).	Yes, third parties and their contribution must be in Annex 1 (EC can still approve if not in Annex 1 (Art 55.)	Yes, third parties and their contribution must be in Annex 1 (EC can still approve if not in Annex 1 (Art 55.)	No (only categories of persons that may receive it).
Bound by the grant agreement	Yes	No	No	No	No	No, but *beneficiaries must ensure that their obligations under Art 35 (Conflict of interest), 36 (Confidentiality), 38 (Visibility of EU funding) and 46 (Liability for damages) also apply to the third parties receiving financial support*, by contractual arrangements *(Art 15.1.2.)*
Operational responsibility	Yes (joint and several in case of multi-beneficiary grant).	No but EC may require joint and several liability with beneficiaries	No	No	No	No, but obligations must be extended by contract *(Art 15.1.2.)*
Financial responsibility	Yes	No	No	No	No	No, but obligations must be extended by contract *(Art 15.1.2.)*
Eligible costs	Costs incurred by the beneficiary and compliant with the cost eligibility conditions set out in the grant agreement.	Costs incurred by the linked third party and compliant with the cost eligibility conditions set out in the grant agreement (same as beneficiary).	Price paid by the beneficiary.	Actual costs for paying the in-kind contribution up to the costs actually incurred by the third party and compliant with cost eligibility conditions set out in the grant agreement.	Costs incurred by the third parties for the contribution (seconded persons, equipment, etc.) and compliant with cost eligibility conditions set out in the grant agreement.	Financial support paid by the beneficiary.
Right of access and audit by the EC, OLAF and Court of Auditors	Yes	Yes, to be ensured by the beneficiary.	Yes, to be ensured by the beneficiary	Yes, to be ensured by the beneficiary	Yes, to be ensured by the beneficiary	Yes, to be ensured by the beneficiary

Appendix B First Open call guide for applicant



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223

Guide for Applicants

Version 1.0

31st October 2020

1 Introduction

1.1 Overview of the Gatekeeper project

Our healthcare systems are detecting conditions and risks when it is too late and once detected, they are not managed properly. The gaps between i) cases diagnosed and cured, ii) diseases and frailty conditions prevented or delayed, is astonishingly high. This means that, as a society, we are currently losing VALUE between what the healthcare system is caring and curing and what the citizens really need.

In this context, innovations could bring support to achieve better diagnosis, treatment and management of citizens across the continuum of care and prevention. However, despite the exponential advances in medical technologies[6] developed and tested on an ongoing basis around Europe, a large proportion are not implemented and never reach citizens. Nowadays, the European Commission is working to provide its citizens access to safe and top quality digital services in health and care, and this process has recently been accelerated by the Digital Single Market initiative, the recent Communication on Digital Transformation of Health and Care in the Digital Single Market, which identified as priorities Citizens' secure access to health data, Personalised medicine through shared European data infrastructure, Citizen empowerment with digital tools for user feedback and person-centred care.

In this sense born Gatekeeper, as an European Multi Centric Large-Scale Pilot on Smart Living Environments which the **main objective** is enabling the creation of a platform that connects healthcare providers, businesses, entrepreneurs, and elderly citizens and the communities they live in, in order to originate an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for the ageing populations.

The **scope** of GATEKEEPER is the application of advanced Information and Communications Technologies (ICTs) to tackle the challenge of improving the quality of life of citizens while demonstrating its significant efficiency gains in health and care delivery across Europe.

The technological platform that will be created in GATEKEEPER for managing all the data and applying digital innovations actions will be crucial. By 2022, GATEKEEPER will be embodied in an open source, European, standard-based, interoperable and secure framework available to all developers, for creating combined digital solutions for personalised early detection and interventions that harness the next generation of healthcare and wellness innovations; cover the whole care continuum for elderly citizens, including primary, secondary and tertiary prevention, chronic diseases and co-morbidities;

[6] Stanford Medicine 2017 Health Trends Report . ht tp://med.stanford.edu/school/leadership/dean/healtht rends.html

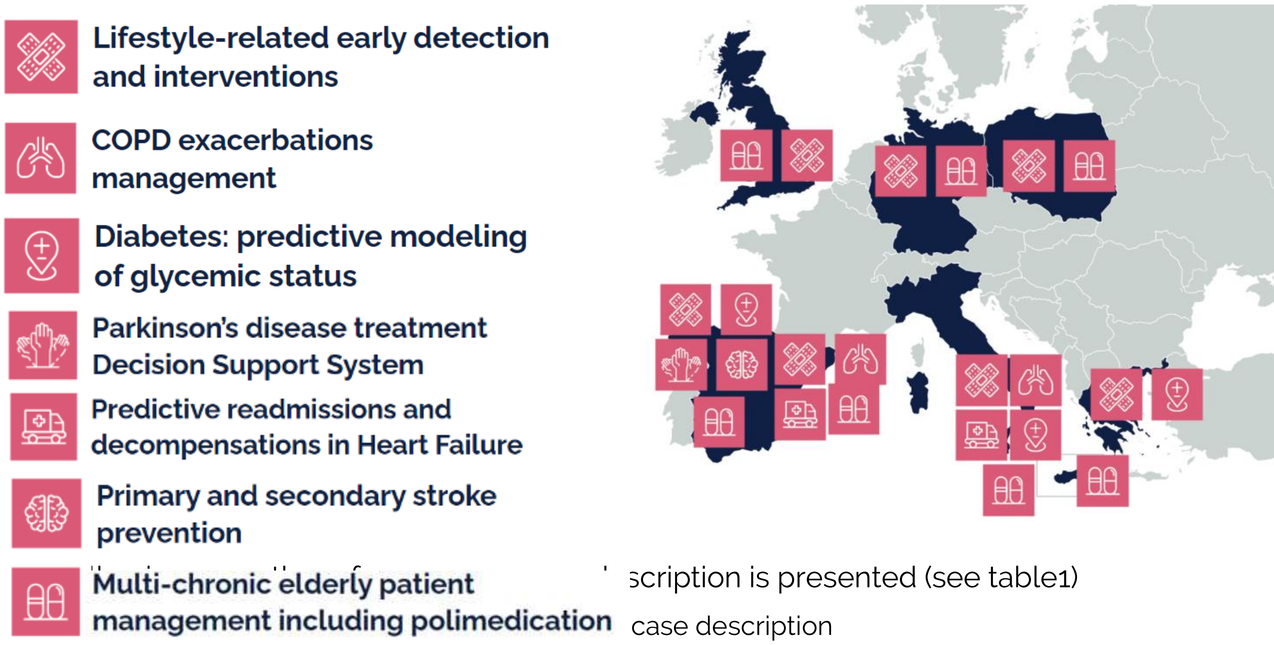
straightforwardly fit "by design" with European regulations, on data protection, consumer protection and patient protection; are subjected to trustable certification processes; support value generation through the deployment of advanced business models based on the Value Based Health Care (VBHC) paradigm.

1.2 Reference use case

GATEKEEPER will demonstrate its value by scaling up, during a 42-months work plan, towards the deployment of solutions that will involve ca 40.000 elderly citizens, supply and demand side (authorities, institutions, companies, associations, academies) in 8 regional communities, from 7 EU member states.

GATEKEEPER Large Scale Pilots (LSP) will establish and consolidate the different Use Cases through Europe enabling the deployment of digital solutions for early detection and intervention and support the risk stratification models. They ensure that GATEKEEPER users' and medical requirements for early detection and intervention are correctly deployed in a coordinated way in all pilot sites.

Figure 19. Pilot and reference use case mapping


Lifestyle-related early detection and interventions
COPD exacerbations management
Diabetes: predictive modeling of glycemic status
Parkinson's disease treatment Decision Support System
Predictive readmissions and decompensations in Heart Failure
Primary and secondary stroke prevention
Multi-chronic elderly patient management including polimedication

Ir scription is presented (see table1)

case description

CASE	THIS CASE	
Lifestyle-related early detection and interventions	▪ Basque Country ▪ Aragon ▪ Saxony ▪ Greece ▪ Puglia	Big Data Analytics techniques will be exploited to address risk stratification and early detection, based on lifestyles analysis including: pattern recognition for the improvement of public health surveillance and for the early detection of cognitive decline and frailty; data mining for inductive reasoning and exploratory data analysis;

	▪ Milton Keynes ▪ Poland	Custer Analysis for identifying high-risk groups among elder citizens. In the above cases timely intervention is provided by through AI-based, digital coaches developed e.g. on top of Samsung AI assistant, Bixby[7] through Natural Language Processing techniques, based structured conversations, consultation and education.
COPD exacerbations management	▪ Basque Country ▪ Aragon ▪ Puglia	Machine learning methods based on Dynamic Bayesian Networks, suitable for modelling knowledge and handing time series data, are added to the Ecosystem Transaction Space to implement apps that predict exacerbations and avoid hospitalizations. These apps will be built on top of advanced wearable monitoring KETs, available in the GK Things Catalogue, that combine, in a single wearable garment piece, time series data for blood pressure, pulse oximetry, ECG, respiration, skin temperature and activity
Diabetes: predictive modelling of glycaemic status	▪ Basque Country ▪ Greece ▪ Puglia	Short-term prediction of glycaemic dynamics is essential to improve Diabetes self-management. GK will provide a personalized, adaptive, real-time data driven computational solution based on data federation in the Healthcare Space, identifying the different modes of the underlying glucose metabolism and eventually prevention, of hypoglycaemic events. Advanced GK "things" will collect clinical data at home such as bio- and physiological signals (i.e. blood glucose concentration data or continuous glucose monitoring data, galvanic skin response, heart rate variability) combining them with adaptive machine-learning regression models.
Parkinson's disease treatment DSS	▪ Basque Country	The medication change model, which was developed in collaboration with medical experts, using a qualitative multi-criteria method, identifies situations in which the

[7] https://www.samsung.com/us/explore/bixby/

		disease has progressed to the point which requires a change of medical therapy and then suggests what kind of changes should be made. GATEKEEPER KETs such as wearable sensors to continuously or periodically measure motor symptoms (depending on disease severity) and digital applications, such as Smart TVs, that can be used to detect non-motor symptoms are used to record data into the patient's EHR, accessible in the GK Healthcare Space. The model will alert clinicians that the patient's current medication plan is not optimal any more, and will derive suggestions on how to improve it.
Predicting readmissions and decompensations in HF	▪ Basque Country ▪ Aragon ▪ Puglia	Telemonitoring services and machine learning with Dynamic Bayes Networks will be harnessed to implement an advanced model for predicting acute HF decompensations, taking comorbidities into account. Building on the experience of the Multisensor Monitoring in Congestive Heart Failure (MUSIC) Trial, GK Healthcare Space apps allow to explore which other longitudinal data (measured by GK Consumer Space "things" , e.g. bio-impedance, heart rate, respiratory rate and volume, physical activity duration and intensity, body posture, gathered with a wearable platform as the one depicted in) can be used for predicting decompensations
Primary and secondary stroke prevention	▪ Basque Country ▪ Saxony	Image recognition algorithms can be added to the Ecosystem Transaction Space, able to detect stroke signs from images recorded at home, for example on the basis of pathological facial weakness detection [24][25]. These algorithms, coupled with smart-home/smart-hospital interactions supported in the GK Healthcare Space, will activate early warning alarms which effectively target secondary stroke prevention, particularly for subjects affected by recurrent strokes. GK "Things" involved in this scenario include image detection technologies (e.g. camera in smartphone) and/or MYSPHERA real-time location system. Primary prevention can be addressed through AI-based smart

		assistants, like Samsung Bixby, aimed at coaching patients on stroke-related healthy habits, similarly, to Use Case 1.
Multi-chronic elderly patient management including polimedication	▪ Basque Country ▪ Milton Keynes ▪ Cyprus ▪ Puglia ▪ Poland	Several sensing technologies, available in the GK Things Catalogue, can be leveraged and integrated in an unobtrusive mobile data collection platform (e.g. based on smartphones, smart-trackers, smart-textiles, etc.), able to monitor the multiple parameters required in Chronic Care Models (CCM) for multi-morbid subjects. Through the GK Healthcare Space, data can be shared with clinical professionals in charge of managing the CCMs, in order to adjust individual care plans accordingly. Through the GK Ecosystem Transaction Space, robotics KETs (from very simple pill dispensers to more complex social robots) can be integrated with digital coaching systems to assist polymedicated patients (e.g. in particular for patients which are concurrently affected by cognitive impairments).

1.3 Objective of the first open call

The objective of the first Open Call is to **engage actively new technology members**, i.e. SMEs, Midcaps and Research technology organizations in the GATEKEEPER Ecosystem**,** **supplying new AI and Big Data applications, tools or components** which will be incorporated in the technology offering portfolio of GATEKEEPER to Pilots and Platform designers and developers.

In concrete terms, the proposals will help to validate different key aspects of the GATEKEEPER project:

- To enlarge and extend new applications and services portfolios on the GATEKEEPER's platform.
- To improve the value of the current services thanks to new or complementary functionalities.
- Attract new players of the ecosystem to become part of the Gatekeeper portfolio ensuring its expansion and sustainability.

2 Application process

2.1 Who can apply?

The call is open to individual **European Industry, MID Cap, SMEs, start-ups, universities, research and technological centers** are willing to contribute to the value based health care paradigm, with the same eligibility criteria of the H2020 rules of participation.[8]

Every participant has to be legally registered in a member state of the European Union or in a Horizon 2020 associated country.[9]

Only **one entity per proposal** will be admitted, so proposals involving multiple partners in co-operation will not be eligible.

GATEKEEPER partners are not eligible for funding and cannot be part of a funded project. We are obligated to avoid conflict of interests, and therefore we reserve the right, at our full discretion, to reject proposal on the basis hereof.

Successful applicants who have been awarded funding will be required to sign the GATEKEEPER Third Parties agreement in order to be able to receive the funds and become third party of the project.

2.2 What are the eligibility criteria?

The submitted proposals must meet the next criteria:

1. Application submitted on time (Deadline: ~~January 29th~~ **February 28th**, 2021, 17:00 CET)

2. Application made by **only one entity** (European Industry, MID Cap, SMEs, start-ups, universities, research and technological centers legally registered in a member state of the European Union or in a Horizon 2020 associated country); activities in co-operation will not be considered eligible.

3. Proposal solutions must provide **solutions based on artificial intelligent and big data.**
4. Completeness of the proposals, **respecting the page limit**.

5. Within the scope of the call, answering **only one of the proposed challenges** of the open call.

7. The language of the applications must be in **English**.

8. GATEKEEPER partners are not eligible for Open Call.

9. Compliance with GATEKEEPER Ethics & Privacy guidelines.

[8] http://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/rules_participation/h2020-rules-participation_en.pdf

[9] http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/international-cooperation_en

2.3 Why should apply?

It is a great opportunity for:

- Offer your solution with a mature ecosystem at European level.
- Access and share knowledge and evidence of benefits of services based on artificial intelligent and big data.
- Better understanding of current needs and gaps of services.
- Access to companies of the key industry in artificial intelligence and big data and relative domains.

2.4 Scope and challenge

The proposals may address one of the challenges listed below and demonstrate how they will implement the solutions in the platform. The complete description of each challenge is available at Annex A - Open Call Challenges (see table 2)

Table 16. Challenge description

#	CHALLENGE	DESCRIPTION
1	Dynamic API injection	This challenge is open to proposals providing plugins for Express Gateway for dynamic APIs
2	Risks detection and timely response (mid-term and time critical)	This challenge is open to proposals providing intervention planners for risks and emergency detection
3	Informal care coordination system	This challenge is open to proposal addressing the coordination of informal careers
4	Increasing insights from HER's un-structured data (risks prevention)	This challenge is open to proposals capable to extract meaningful information from EHR´s convertible into actionable insights
5	Robot companions against social isolation	This challenge is open to proposal addressing the design and development of robotic platforms
6	Embedded ML[10] in Smart Devices	This challenge is open to proposal addressing the design and development of innovative prototypes of hardware /software solutions.

[10] ML, Machine learning

2.5 Information requested in your proposal

Proposals are submitted in a one-stage process that means that applicants submit a full proposal prior to the deadline. The proposal language is English. Proposals submitted in other language will not be eligible.

The GATEKEEPER consortium has prepared an application toolkit that the interested entities must use (download in this link). This toolkit includes the proposal template (word document) and budget project (excel file).

The information requested in your proposal are the next:

Organization background and details:

- Title of your contribution, identification of organization, contact person and declare you are non-affiliated with GATEKEEPER partners.
- The organization profile and key member's CV, organization, skills and resources applicants have.

Proposed solution:

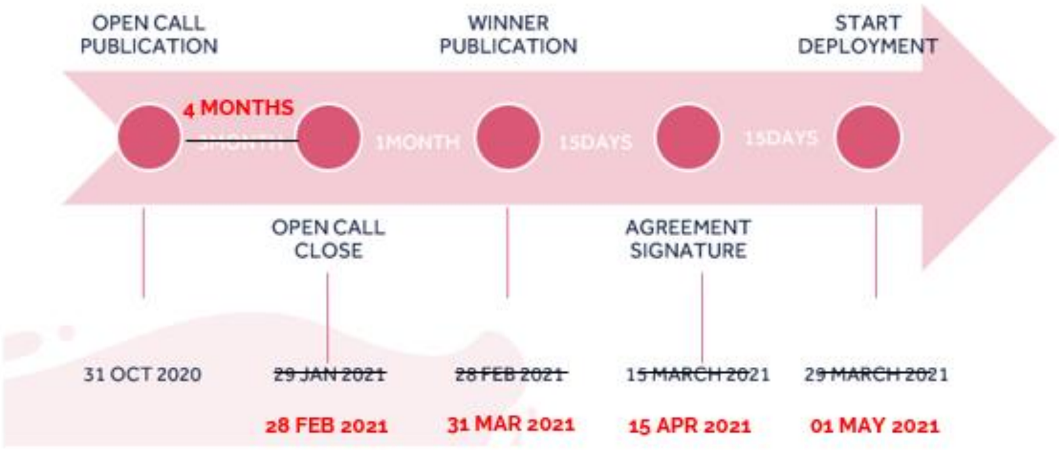
- Description of the contribution and the objectives, relating to the GATEKEEPER approach, and how the proposed collaboration may fit into Gatekeeper vision and help to add value to the project.
- A list of activities and their time plan aligned with the experimentation period – activity will be held from ~~March 2021 to March 2022~~ **May, 1st 2021 to April, 30th 2022** (12 moths). Please explicitly list what are considered to be the key milestones and deliverables within this plan, considering also the alignment with the internal evaluation periods.

Budget plan (budget excel file):

- The budget for cost related to the funding proposal.
- Upload your budget for the project using the template provided by the GATEKEEPER Consortium (available in the "Application toolkit").

2.6 Timeline and key steps for application

Figure 20. Timeline Open Call



The funded projects will start in ~~March 2021~~, **May, 1st 2021** and they will have a total duration of 12 months, **ending on April, 30th 2022**

This timetable could be amended as required at the GATEKEEPER team discretion. The most updated version will be available on GATEKEEPER website.

The main steps of the submissions are the next:

1. Registration at the GATEKEEPER web page.

Register your interest and download all the required information and Open Call templates:

www.gatekeeper-project.eu/open-call

2. Submit application by 17:00 h (CET) on 29th January 2021

Prepare your applications material and submit them to the Open Call web portal.

https://gatekeeperprj.beinformatica.com/

3. Sign legal documents.

All applicants will receive a notification by February 2021. Successful applicants will receive final notification and a request for signing the Third Parties Agreement.

3 Evaluation process

3.1 Who will evaluate my proposal?

Every proposal will be checked to ensure that it meets requirements before it is sent for evaluation to the Open Call Review Board (OCRB). This board consists of an external and independent group of experts, who will be monitoring the whole process to ensure tracking of every action.

The experts will be individuals with experience in the fields of innovation linked to this Open Call and also with the highest level of knowledge. They will sign a declaration of confidentiality concerning the evaluation process and the content of the proposals they evaluate. They will also declare their absence of any conflict of interest for the assigned tasks.

Each proposal will be evaluated anonymously by 2-3 reviewers. Each evaluator will record his/her individual opinion on each proposal using the web portal. A ranking list will be assembled with all proposals that score above the threshold (per individual category and total)

Each external expert will assign a score between 0 and 5 to each of the criteria mentioned below. The assigned scores of the experts will be averaged for each criteria to get one single score for each criteria. A total score of a proposal is reached by calculation the sum of all individual scores of the evaluated criteria of a proposal.

Notifications on funding or rejections will together with any feedback be sent out by February 2021.

3.2 What does evaluation measure?

The proposals will be evaluated under the following criteria:

4. **EXCELLENCE:** Soundness of concept, quality of objectives and innovative elements present in the proposal. Max=5. Threshold =3
   - How well does the proposed solution address the challenge as detailed in the open call text?
   - Are the proposed objectives clear and pertinent?
   - Is the concept sound and shows a clear plan for development of a working solution?

5. **IMPLEMENTATION:** quality and efficiency of the implementation and the management. Feasibility of the workplan, quality and effectiveness of the technical methodology, including the workplan, contribution to collaboration with Gatekeeper to achieve objectives of the project, appropriateness of the allocation and justification of the resources to be committed (staff, equipment…) Max=5 Threshold =3
   - How effectively will be the Application Experiment be managed? Is the proposed work plan coherent and effective?

- Are deliverables, milestones and deadlines defined and adapted to the goals of the proposals?
- Is the allocation of tasks and dedicated resources (e.g. human capital, equipment, man hours, etc.) appropriate and necessary to necessary to perform the scope of the proposal and achieve its objectives?
- Are the costs clearly defined and aligned with the required efforts?
- Does the third party possess the technical skills and abilities necessary to perform the scope of the proposal?

6. **IMPACT AND SUSTAINABILITY**: Potential impact through the development, dissemination and use of project results, in which way the proposal contributes to further maturity, integration and interoperability of gatekeeper AI solutions, and explain if you consider any further support after your participation in Gatekeeper project. Max=5 Threshold =3
   - Does the proposal enhance innovation capacity and the integration of new knowledge?
   - Assessment of resources required to demonstrate you have taken into account all key elements for the success of your project to reach exploitation.
   - Strategic fit for the company explaining why this project is important for your company.

Each category will be scored on a scale from 0 to 5, with excellence and implementation having double weight, and impact and sustainability having single weight; thus, the overall maximum score is 25. For a proposal to be considered for being selected for funding, the score has to pass a threshold of 3 out of 5 in each individual category (for the double-weighted impact, this means a score of at least 6 out of 10). The total sum of the individual scores must reach the minimum threshold of 20 points.

The individual scores have the following interpretation:

0 - Fail: The proposal fails to address the criterion under examination or cannot be judged due to missing or incomplete information.

1 - Poor: The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.

2 - Fair: While the proposal broadly addresses the criterion, there are significant weaknesses.

3 - Good: The proposal addresses the criterion well, although improvements would be necessary.

4 - Very good: The proposal addresses the criterion very well, although certain improvements are still possible.

5 – Excellent. Proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

The selected proposals will be reported to the gatekeeper project officer of the European Commission for a final granting decision

3.3 Communications with applicants.

After the evaluation of the proposals all proposers will be informed if their application experiment was accepted or not.

Members of Gatekeeper project will get in contact with the successful applicants to prepare the conclusion of third-party agreements.

4 Funding Conditions

4.1 Budget available

The first open call will give **600.000 €** in funding, with a **maximum of 60.000€ for each project**. GATEKEEPER project may fund a **maximum of 10 third party** projects.

Each project will include an implementation plan including milestones and deliverables, and a cost estimate justifying the costs and resources in relation to the implementation plan. The estimated costs of the third party should be reasonable and comply with the principle of sound financial management in particular regarding economy and efficiency.

Other important information that you need to know:

- The **industrial** third parties will be **funded 70%** of their respective cost.
- The distribution of funding over time will be: up to **20% of pre-financing** at the start; an **interim payment of 50%** and a **final payment** up to 100% of the total funding. Each funding stage will be paid upon approval of the Project Agreement (which includes the project plan), and the approval of interim and final reports respectively. Each payment is released 30 days after the approval of each report.
- Indirect cost (e.g. overheads) will be covered if they are declared as flat-rate of **25% of the eligible costs**.
- The third party cannot request any funding for activities that are already funded by other grants (the principle of no double funding).
- The reports require the candidates to provide GATEKEEPER with honest feedback on their project and their experience of the technical environment.

The expected duration of an Application Experiment is 12 months.

4.2 Which costs are you allowed to include in your budget?

You are eligible for funding for all activities mentioned below, under the condition that these activities take place after the approval of the Third Parties Agreement and contribute to maturing, sustaining, and further developing GATEKEEPER and follow the guidelines below:

1. Planning and execution of the Project
2. Technical integration and adaptation, and project deployment on the GATEKEEPER technical environment.
3. Generation of reports and publications related to the projects, including preparation of a showcase about the project that can be used for dissemination purposes.
4. Supporting the rest of technical activities in the project, by providing feedback about the use of the technical framework and identifying gaps of the development of appropriate standards.
5. Report the necessary effort and costs according to H2020 rules and management practices requested by the GATEKEPEER open call lead partner.

For a cost within your project to be **eligible** for funding it must:

- Be incurred and paid between your project start and end dates, as specified in our legal agreement
- Be directly related to the activities listed previously
- Be indicated in the estimated budget
- Be incurred in connection with the action as described in your project application and necessary for its implementation
- Be identifiable and verifiable, in particular recorded in your accounts and in accordance with the accounting standards applicable in your country and according to your organization's usual cost accounting practices.
- Comply with the applicable national law on taxes, labour and social security.

You are allowed to include:

- Staff costs.
- Subcontracting costs.
- Material costs.
- Travel costs.
- Other cost.

"**Ineligible costs**" are:

- Costs that do not comply with the conditions set out above and
- Costs reimbursed under another EU or Euratom grant (including grants awarded by a Member State and financed by the EU or Euratom budget and grants awarded by bodies other than the European Commission for the purpose of implementing the EU and Euratom budget).
- The form of financial support to be used will be a pre-defined lump sum. Funds will be provided to the third parties following the accomplishment of different milestones verified on the basis on the presentation of technical and financial reports.

Regarding staff costs, the eligible labour costs will be salary amounts actually incurred a paid (monthly/hourly). Note that the number of working days per year for the organisation is based on full time working days per year, less standard holiday allowance. Sick days, waiting time, training days and non-produce time are not eligible as part of the salary calculation.

For more information about personnel costs, see H2020 – AGA, Article 15 – Financial support to third parties.

Regarding subcontracting costs: if necessary, to execute the project, you may subcontract part of the activities in the project. Subcontracting may cover only a limited part of the project. For more details about subcontracting costs, see H2020-AGA, Article 13.

The total amount of time and cost will be reviewed before approval for funding. The reviewers can decide to fund your proposal with a reduced amount.

5 Who keeps the IPR?

Successful applicants will become Third Party of the project. You and your project will be sole owner of the enabled solution of your project. However, GATEKEEPER Consortium will be licensed the right to use (internally) and IPR you produce as part of the project, for three years after the project finishes.

GATEKEEPER project itself will not retain an equity stake in your company, not will it retain any IPR.

Additionally, GATEKEEPER or the European Commission may ask you to present your work as part of our public relations and networking events, in order to showcase the benefits of the GATEKEEPER project.

5.1 Who owns the data produced?

The type of data available for GATEKEEPER Open Call projects is manifold, representing the contextual diversity of smart environments which mirrors the complex reality of the active and healthy ageing market. The type of data that you may make use of could be open data and close data, with either open access or restricted access. Each pilot has its own data policy and preferences on how data should be treated in their framework.

It will be the responsibility of the applicants to ensure that they understand the conditions on data in each pilot, as well as associated licences and costs, in order to provide a sound proposal that takes this diversity into account. It will be also the responsibility of applicants to propose data processing solutions compliant with the current GDPR.

As a guideline, the IPR of the data collected previous to the GATEKEEPER Open Call will remain the property of the data provider or its licensors. The data produced during the pilot phase will be shared according to the contractual Data Sharing Agreements between the winning applicants and the pilot.

6 Support options

The GATEKEEPER consortium maintain a frequently asked questions (FAQ) section available in www.gatekeeper-project.eu/open-call. It will be updated continuously. For especially technical details check first the available documentation in the website.

The answers that you cannot find in the FAQ section can be submitted by contacting opencall@gatekeeper-project.eu Here you can get support regarding technical matters or the proposal.

There will be different events in which the open call will be presented, and support will be provided in preparing the applications. Follow the web site and the social networks accounts of the project to get information about the open call.

7 Summary of revisions

version	Sections update	Date updated
V3.0	Section 2.2 Submission deadline **February 28th** instead of January 29th	22th December 2020
V3.0	Section 2.5 Dates of starting and ending project **May, 1st 2021 to April 3oth, 2022** instead of March 2021 to March 2021	22th December 2020
V3.0	Section 2.6 New dates (red color) included in the **figure 2**	22th December 2020
V3.0	Section 2.6 changed dates. The funded projects will start in **May, 1st 2021** and they will have a total duration of 12 months, **ending on April, 30th 2022**	22th December 2020
V2.0	Section 7 summary of revision added	04th December, 2020
V2.0	Section 2.2 Submission deadline January 29th instead of Januaty 28th	04th December, 2020
V2.0	Section 2.5 Dates of starting and ending project March 2021 to March 2022 instead of March 2020 to February 2021	04th December, 2020

Appendix C Open call challenge

#	CHALLENGE	DESCRIPTION
1	Dynamic API injection	The combination of technologies such as containers and orchestrations allow horizontal (replication of services) and vertical (improvement of resources) scalability of a digital platform. These features are the basis for the automatic growing up of a platform and serverless infrastructures. An important technology used in Gatekeeper is the Express API gateway that provide isolation and load balancing in a microservice architecture. This challenge is open to proposals providing plugins for Express Gateway for dynamic APIs that are designed for the injection of novel services without rebuilding the system or hot reloading of the gateway configuration. The solution should be able to develop and implement a set of plugin for Express Gateway based on: 1. The automatic provisioning and injection of novel services into an existing platform 2. The automatic configuration of the platform in terms of novel available services 3. The maintenance of the reliability of the new increased platform against previous one. An existing digital platform has to take advantage of this added value, that enables a transparent growth of API services and infrastructure, that should be demonstrated by adding tens of services maintaining the initial performance benchmarking of the platform (e. g latency, network throughput, reliability, etc..). **TRL ≥ 8**

#	CHALLENGE	DESCRIPTION
2	Risks detection and timely response (mid term and time critical)	The combination of data from home & personal devices (including healthcare and consumer devices), digital solutions, the predictive models and the health profiling of elders dramatically increase the possibility to identify risks and emergency events (even in real-time). Some risks and emergency events are time sensitive. The prolongation of risks can trigger a worsening of elder conditions or an emergency event, such as obstacles can result in a fall or a prolonged isolation can lead to depression. Similarly, emergency events require a fast assessment of the real conditions of the elder and its severity to evaluate the best course of action, for instance a fall can cause a minor or a major injury or could be the result of a cardiac event. This challenge is open to proposals providing intervention planners for risks and emergency detection, able to translate the input from AI services into time-sensitive operational plans of intervention based on the available resources, aimed to assess the real conditions of the elder or to trigger the intervention of carers or emergency units. The solution should be able to develop and implement a timely strategy based on: ▪ The available guidelines for the type of event ▪ The reliability of the results given the available information (confidence of the detection) ▪ The configuration of the system in terms of available "actuators", such as the opening times of the healthcare services, proximity of family members, remote cameras or other communication devices In this challenge GK Consortium will contemplate proposals tackling one of the following scenarios: ▪ Time Critical Emergency Detection and Timely Response: Focused on monitoring of acute events in clinical conditions considered time-critical (Stroke, Heart Attack, Critical Arrythmias, Hypoglycemia, etc.) ▪ Mid-Long Term Risk Detection: More oriented to Chronic conditions and mid/long-term risks associated to them (complications or risk of comorbidities) such as Diabetes decompensations, Cancer, COPD, Fragility, etc. This solution is the cornerstone for transforming monitoring and communication technologies in infrastructures for ubiquitous care. Indeed, new monitoring and communication technologies are transformed into medical devices thanks to data-driven algorithms. While the efficacy of these devices is often life-saving, their impact on mild conditions and small events is limited to "nudging" a behavioral change from the user. In this view, the identification of risks and events combined with clear, verified instructions for informal,

		untrained carers and for the end-user transforms the consumer technology ecosystem of the user as a whole into an enabler "intervention" technology. The qualitative change of the technology system as an intervention technology for informal carer multiplies the efforts and outreach of the national healthcare system and healthcare professionals beyond the silos of specific care and technological providers. **TRL ≥ 6**

#	CHALLENGE	DESCRIPTION
3	Informal care coordination system	Carrying activities mostly relies on non-professionals, informal carers, such as family members, friends, neighbors, volunteers. Differently from professional carers, informal carers are not trained, they cannot rely on coordination mechanisms of a professional settings and their carrying responsibilities could be unreliable as the result of the balancing with work and other activities. This challenge is open to proposal addressing the coordination of informal carers with the aim of providing a light weighted communication solution to support practical challenges about sharing the responsibility of carrying, such as the frequency of visits, support to routinely activities and timely intervention in case of emergency and need. The expected outcome of a solution should be ability to: 1. profile and monitor informal care activities, 2. supporting a dynamic, transparent scheduling and re-scheduling of tasks involving carers and elders 3. enabling the bi-lateral communication of the GATEKEEPER services for: o Log information for the evaluation by professional carers o Requests interventions triggered by early-detection and predictive algorithms Informal care is currently recognized a central role in the wellbeing and resilience of elders and communities. On the other hand, the lack of formal structures and monitoring configures a friction between formal and informal caring services and resulting duplication of efforts, costs and overall heterogeneous accessibility to caring. As result of the COVID-19 pandemic, the UK government included informal care in the national response strategy bootstrapping a process of rethinking the relation between the national healthcare system and the local organizations. In this scenario, the solution should fill the gap between the formal service management structure and the local self-organized community caring enabling the fully realization of the government vision for an integrated NHS community-based care. **TRL ≥ 6**

#	CHALLENGE	DESCRIPTION

4	Increasing insights from HER's un-structured data (risks prevention)	Electronic Health Records and other clinical resources contain valuable information, currently mostly underutilized by Big Data and AI technologies, mainly because they are un-structured and written in Natural Language. In this challenge, we are looking for solutions capable to extract meaningful information from EHR´s convertible into actionable insights (algorithms, alerts, new variables to monitor, clinical pathway process re-engineering, risk factors, dynamic care plans, patient phenotype classification, etc.) oriented to the prevention and/or prediction of risky situations in a specific clinical pathway or even the generation of new research hypotheses. The clinical pathways tackled by each proposal must be be clearly specified, as well as the expected output and outcomes of the analysis. One proposal may address more than one clinical pathway. Proposals in this challenge combining the analysis of structured and un-structured data will be considered positively. **TRL ≥ 6**

#	CHALLENGE	DESCRIPTION

5	Robot companions against social isolation	Robot companions are a family of social robot specifically meant to provide comfort to users by mimicking pets. This type of intervention is being assessed as effective in mitigating the effects of isolation and loneliness while combining monitoring and alternative modality of communication via robotic interface. On the other hand, the currently available products are based on custom platforms and software configuring a close environment and costly solutions not fitting an open ecosystem as the GATEKEEPER nor the need for scalable solutions to tens of thousands on elders living alone. This challenge is open to proposal addressing the design and development of robotic platforms based on open standards hardware and software and based on the GATEKEEPER services. The expected outcome of a solution should be ability to: 1. Communicate with the user through physical cues based on external services such as Samsung's Bixbi and other conversational AI systems that could be integrated in the GATEKEEPER ecosystem, 2. Identify medical events and provide basic healthcare and wellbeing services, such as coaching, reminders and alerts based on the GATEKEEPER AI services 3. Provide an open abstract interface to the GATEKEEPER service for interacting with the user, such as remote control, sensors streaming and voice command, connecting the robot companion with the service ecosystem and the user medial and smart home devices The development of an affordable, open robot companion based on an ecosystem of services is expected having a disruptive effect. Indeed, the current solutions are outside the possibility of most of the potential beneficiaries, elders living alone that can benefit from a robot companion. Not only this solution can have a disruptive effect in the access to robot companion but also in terms of their potential impact. Current solutions are based on close / single-provider ecosystem of services limiting their integrability within a wider technology and service ecosystem and, in general, the quality of the services available through the robotic platform. In this view, this solution should provide a compelling offer of cutting-edge services and flexibility of use in multiple configurations of healthcare devices, smart home devices and wearable fitting the user needs and living conditions. **TRL ≥ 6**

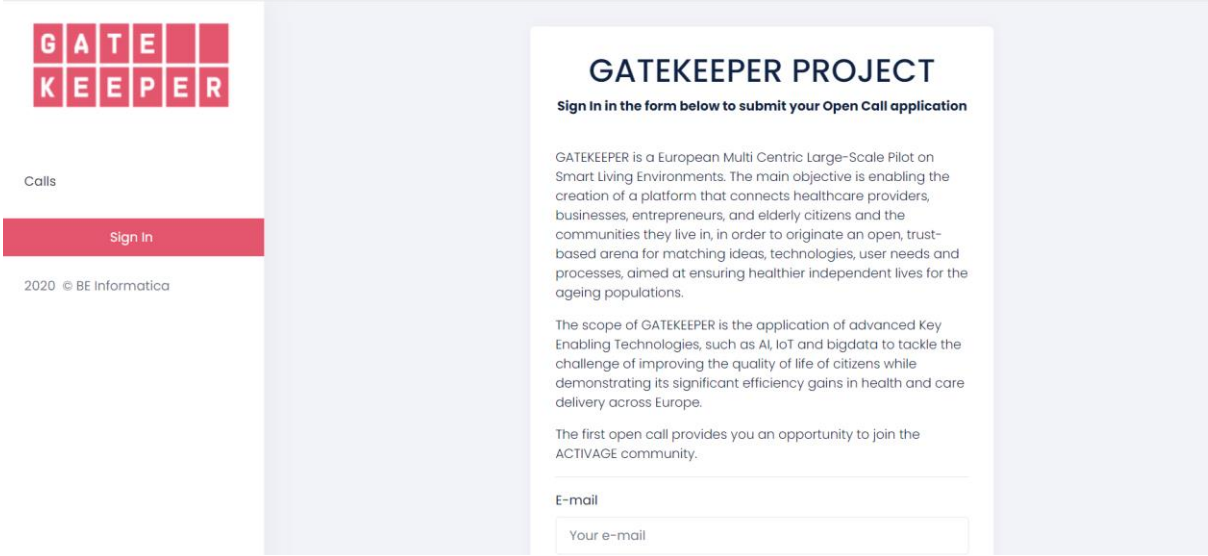
#	CHALLENGE	DESCRIPTION

6	Embedded ML in Smart devices	The growing capacity of producing data by individuals and by the environment where they live is producing new requirements of moving computing capacity from the cloud to the edge. Indeed the Edge Computing is nowadays a generalized trend in almost all sectors of IoT, from industry to environment, energy, farming and may others. In the health care sector, edge can be defined as the space close to the individual where he/she live and move around. For instance, the home, but also the body environment, a neighbourhood, public spaces or other similar. Edge computing is meant to provide efficient data processing, including AI capabilities for faster detection, saving of communications resources, energy, and enhancing data security and privacy, among others. All these features are relevant for GATEKEEPER This challenge is open to proposal addressing the design and development of innovative prototypes of hardware/software solutions able to embed ML algorithms for early detection of vital parameters and life conditions, using real time and time-aggregated data produced by the user and its environment, with strong requirements in term of interoperability (communication using various wireless protocols) and/or cybersecurity (data, AI and privacy protection) among others. At least two use cases are needed to implement, for instance, but not limited to: a) advanced medium-long term behavioural changes detection based on activity detection and performance, b) mental condition: mood, isolation, social connectivity, anxiety, or other. More use cases will be positively evaluated. Data sources and data types must be identified the output parameters as well for all use cases. Re-use of data across use cases is a desired feature. The proposal must describe training and validation approaches and identify data sets used. Working prototypes, either on wearable device, gateway and or any other smart device (TRL6), must be provided for evaluation in laboratory tests and in real working conditions in one or more pilots in GATEKEEPER. TRL ≥ 6

Appendix D Application Submission Guide

D.1 How to submit your application for open call?

1. Go to the link: https://gatekeeperprj.beinformatica.com/



GATEKEEPER PROJECT

Sign In in the form below to submit your Open Call application

GATEKEEPER is a European Multi Centric Large-Scale Pilot on Smart Living Environments. The main objective is enabling the creation of a platform that connects healthcare providers, businesses, entrepreneurs, and elderly citizens and the communities they live in, in order to originate an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for the ageing populations.

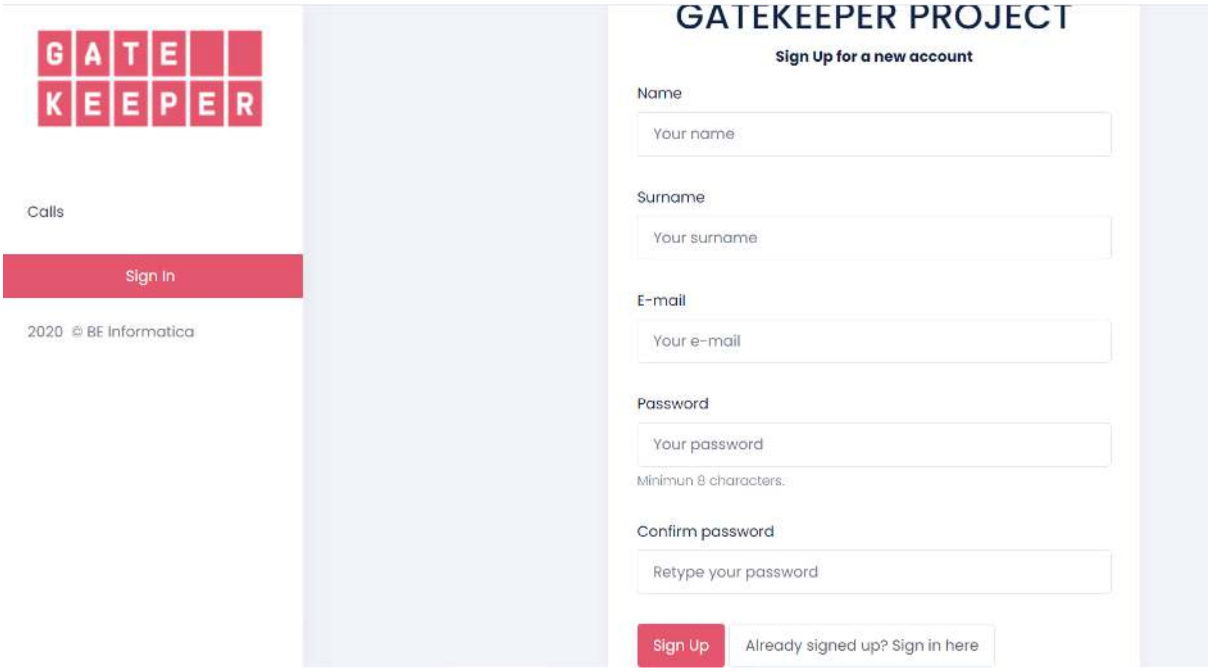
The scope of GATEKEEPER is the application of advanced Key Enabling Technologies, such as AI, IoT and bigdata to tackle the challenge of improving the quality of life of citizens while demonstrating its significant efficiency gains in health and care delivery across Europe.

The first open call provides you an opportunity to join the ACTIVAGE community.

E-mail

Your e-mail

2. Create an account on the platform



GATEKEEPER PROJECT

Sign Up for a new account

Name

Your name

Surname

Your surname

E-mail

Your e-mail

Password

Your password

Minimun 8 characters.

Confirm password

Retype your password

3. Login to your account
4. Submit your proposal

Appendix E Ethics & Privacy guidelines

E.1 Ethics guidelines

Compliance with ethical requirements is cherished in the GATEKEEPER project. Applicants will be required to sign an Ethical statement during application requiring self-disclosure of matters such as past professional misconduct – as well as a guarantee of future compliance with ethical and legal principal under the GATEKEEPER project.

All participants in the project are expected to consider ethics issues throughout its lifecycle – before, during, but also after the pilot period in relation to knowledge exchange and impact activities (such as reporting and publication).

Below are a set of core ethical principles providing general guidance that the winning applicants will need to follow:

1. Respect for general personal data protection principles according to the European GDPR law, by design and by default.
2. Projects should be conducted with integrity and transparency.
3. Lines of responsibility and accountability should be clearly defined.
4. Independence of projects should be maintained and where conflicts of interest cannot be avoided they should be made explicit.
5. The rights and dignity of individuals and groups should be respected.
6. Data subjects' rights exercise to be informed, to object, to be forgotten, and to withdraw consent should be ensured.
7. Personal data processing should be conducted in a lawful way.
8. Decisions based solely on automated processing of data should be avoided.
9. Processing of data that may profile data subjects should be excluded.
10. Processing of genetic data, biometric data, data concerning health of data concerning a natural person´s sex life should be excluded.

E.2 Privacy Policy

All data collected and/or processed within GATEKEEPER project will need to be compliant with the GDPR regulation. In this respect, the GATEKEEPER Open Call will involve:

1. Collection of personal and non-personal data from the open call applicant.
2. Collection and processing of deployment site related data by the winning.

E.3 Collection of personal & non-personal data from the open call applicant

By inviting participants to submit a pilot project proposal the GATEKEEPER Consortium will collect the participant's personal data submitted by them and processed in accordance with applicable law and data protection with particular regard to the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (infra "GDPR"). The processing of your personal data, your privacy and your rights will be based on the principles of fairness, lawfulness, transparency, integrity

E.4 Nature of data collected

You can participate in the open call by submitting your details through the online platform. Through this submission GATEKEEPER collects personal data: family name, first name, country of residence/registration, personal email address, phone number and the relevant registration number allocated to your application.

E.5 The purpose and modalities of the processing for which the data are intended

Your personal information, referring to you as a natural person, or related to the company that you represent, is collected for the purpose of checking the eligibility for funding of the applicants and for the purpose of the obligatory reporting by GATEKEEPER to the European Commission.

Your personal data may be processed both by digital and non-digital means, with full respect of the security measures provided by the GDPR.

Additionally, during the project period the winning applicants can be asked to participate in interviews or to contribute to communication material on their pilots. Such material, including personal data, will be published in GATEKEEPER social media channels, the GATEKEEPER website or communicated through relevant press releases.

Finally, we may use the personal data you provide to contact you after the end date of the project, to inform you of similar initiatives and invite you to participate in new activities. For these purposes, we may contact you by email.

We take the security of your personal data seriously and we have followed a privacy-by-design architecture in order to ensure that your data is secure at all times.

E.6 The obligatory or voluntary nature of providing the requested data and the consequences of a potential refusal of providing such data

Providing your personal data for the purpose of registration and submission of your project proposal is not compulsory, yet the refusal to provide such data will preclude you from participating, as it will render you ineligible to receive the grant.

Providing your data for the promotional and marketing purposes described above is optional and requires the relevant prior consent, that you may give by clicking the checkbox in the application form on the platform used. In the absence of such consent you can still participate in the project, however, the GATEKEEPER Consortium cannot send you any further information about similar activities after the conclusion of the project. Your consent, once provided, can be revoked at any time for all the contact modalities (whether traditional, such as paper-based mail, or automated, such as sms or e-mail), as well as only for one or some of them, by submitting a communication to the Data Controller, without any formality, at the following email address: opencall@gatekeeperproject.eu.

E.7 Entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data

After your personal and identifying data is anonymised by GATEKEEPER, your remaining data from the open call application will be shared with the open call reviewers, who will sign a Declaration of absence of Conflict of Interest prior to the revision. Your proposal will be also shared with the Project Steering Board made of selected members of the GATEKEEPER project. All the organisations involved in the revision of the open call application will be considered as Data Processors.

For the purposes of the competition, if you are selected for the grant, your company name will be published on the GATEKEEPER website together with the name of the project and funding amount (in compliance with EC guidelines for Cascading funding).

E.8 Your rights of access to, and rectification, of your data

We remind that, in your capacity of natural person, you can exercise your rights against the GATEKEEPER Consortium at any time, in accordance with the relevant provisions of the GDPR, by sending an email without formality to opencall@gatekeeper-project.eu.

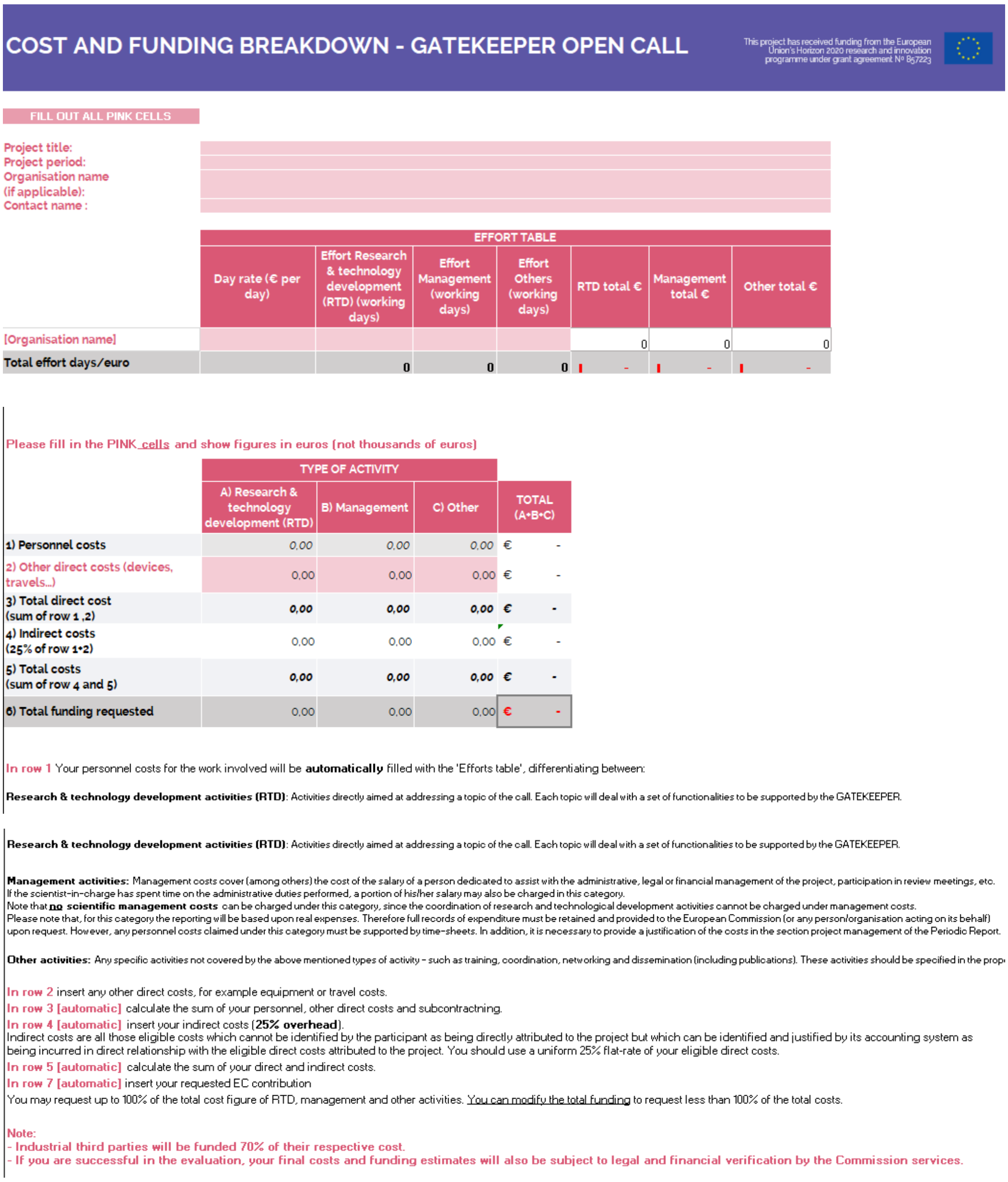
It is important to notice that the open call participants will be the ultimate responsible for the compliance with the GDPR rules.

For this reason, we recommend the following:

- SMEs looking to comply with the GDPR should first carry out a data audit in order to establish factual context such as: what data the company holds, where it is held, third parties who have access, retention issues, security etc.
    - Applicants should make sure that decision makers and key people in their organisation are aware that the law changed to the GDPR in May 2018 and they need to understand the impact this is likely to have.

- Applicants should review the current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
- Applicants should check the procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
- Applicants should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Appendix F Budget template



COST AND FUNDING BREAKDOWN - GATEKEEPER OPEN CALL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 857223

FILL OUT ALL PINK CELLS

Project title:
Project period:
Organisation name (if applicable):
Contact name :

	EFFORT TABLE						
	Day rate (€ per day)	Effort Research & technology development (RTD) (working days)	Effort Management (working days)	Effort Others (working days)	RTD total €	Management total €	Other total €
[Organisation name]					0	0	0
Total effort days/euro		0	0	0	-	-	-

Please fill in the PINK cells and show figures in euros (not thousands of euros)

	TYPE OF ACTIVITY			
	A) Research & technology development (RTD)	B) Management	C) Other	TOTAL (A+B+C)
1) Personnel costs	*0,00*	*0,00*	*0,00*	€ -
2) Other direct costs (devices, travels...)	0,00	0,00	0,00	€ -
3) Total direct cost (sum of row 1 ,2)	***0,00***	***0,00***	***0,00***	**€ -**
4) Indirect costs (25% of row 1+2)	0,00	0,00	0,00	€ -
5) Total costs (sum of row 4 and 5)	***0,00***	***0,00***	***0,00***	**€ -**
6) Total funding requested	0,00	0,00	0,00	€ -

In row 1 Your personnel costs for the work involved will be **automatically** filled with the 'Efforts table', differentiating between:

Research & technology development activities (RTD): Activities directly aimed at addressing a topic of the call. Each topic will deal with a set of functionalities to be supported by the GATEKEEPER.

Research & technology development activities (RTD): Activities directly aimed at addressing a topic of the call. Each topic will deal with a set of functionalities to be supported by the GATEKEEPER.

Management activities: Management costs cover (among others) the cost of the salary of a person dedicated to assist with the administrative, legal or financial management of the project, participation in review meetings, etc.
If the scientist-in-charge has spent time on the administrative duties performed, a portion of his/her salary may also be charged in this category.
Note that **no scientific management costs** can be charged under this category, since the coordination of research and technological development activities cannot be charged under management costs.
Please note that, for this category the reporting will be based upon real expenses. Therefore full records of expenditure must be retained and provided to the European Commission (or any person/organisation acting on its behalf) upon request. However, any personnel costs claimed under this category must be supported by time-sheets. In addition, it is necessary to provide a justification of the costs in the section project management of the Periodic Report.

Other activities: Any specific activities not covered by the above mentioned types of activity - such as training, coordination, networking and dissemination (including publications). These activities should be specified in the prop

In row 2 insert any other direct costs, for example equipment or travel costs.
In row 3 [automatic] calculate the sum of your personnel, other direct costs and subcontractning.
In row 4 [automatic] insert your indirect costs (**25% overhead**).
Indirect costs are all those eligible costs which cannot be identified by the participant as being directly attributed to the project but which can be identified and justified by its accounting system as being incurred in direct relationship with the eligible direct costs attributed to the project. You should use a uniform 25% flat-rate of your eligible direct costs.
In row 5 [automatic] calculate the sum of your direct and indirect costs.
In row 7 [automatic] insert your requested EC contribution
You may request up to 100% of the total cost figure of RTD, management and other activities. You can modify the total funding to request less than 100% of the total costs.

Note:
- Industrial third parties will be funded 70% of their respective cost.
- If you are successful in the evaluation, your final costs and funding estimates will also be subject to legal and financial verification by the Commission services.

Appendix G Technical information

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 857223

Platform Overview

Version 1.0
31st October 2020

Abstract

Gatekeeper platform is a digital platform that provides AI and data-oriented services for the development of health and care solutions.

Gatekeeper is based on the concept of digital twin where every platform asset, such as devices, services, data or even if other platforms, has a digital replica that is described with a Thing Description in agreement with Web of Thing standard specification.

Within Gatekeeper the Things are virtual entities that are, decoupled but linked with their physical and/or technological implementation. Based on that at data level Gatekeeper allows a high degree of separation between data owner (the physical owner of a database for instance) from the data provider (the service that wraps the data into a digital twin).

The Gatekeeper core data are the data related to the Gatekeeper users. Gatekeeper users are developers and customers, nor patients neither healthcare professionals are expected to be Gatekeeper user.

Anyway, when a developer builds an application by using Gatekeeper services he can associate to several Gatekeeper services sensible data such as personal patients' and/or healthcare professionals' data. This data are private data owned by the developers that Gatekeeper is hosting and for which is granting security and privacy implemented into the platform and the deployment infrastructure. Data stored into the Gatekeeper platform associated with a user are isolated from any other user.

Data belonging to a developer are only accessible and visible by that developer. For the applications developed on the top of the Gatekeeper services, the developer is responsible to implements the adequate privacy and security mechanisms to avoid data breaches to his applications by using appropriate countermeasures.

Anyway, developers can rely on some core security and privacy services provided by Gatekeeper that can help them to do this job, such as standard user management services for custom authentication and authorization, secure connections and communications provided by Gatekeeper infrastructure services, intrusion detection systems (IDS) for network traffic generated by developers' applications, etc.

Furthermore, Gatekeeper can provide to pilot developers some additional feature in terms of a federation of their physical resources (not only data) into the Gatekeeper platform.

The Gatekeeper platform by default is deployed into the data centre provided by HPE in Rome. Such data centre provides both physical security (security personnel, access control to the facilities, locks of the physical infrastructure) either IT security such as above-mentioned services IDS, etc. Based on that, the storage and data extraction operations are physically done into the HPE data centre.

1 Architecture definition principles

This document describes GateKeeper reference architecture. The main goal is to help the platform component owners to collaborate effectively, having a coherent view of the platform as a whole, a detailed description of the main components needed for the implementation of the GateKeeper platform and the interaction expected between these components to satisfy the requirements coming from Technical Requirements as well as Pilots (WP6), and other user requirements (WP2). In this first section we will describe the defining principles that drive the design of the Gatekeeper Platform, then we introduce the stakeholder of the platform and an overview of the target cloud infrastructure, as well as security and privacy concerns.

1.1 Web of Things

Gatekeeper platform will be based on the Web of Thing (WoT) layered architecture described in **Error! Reference source not found.**. The main difference between the Gatekeeper layered architecture and the WoT layered architecture relies on the inclusion of an additional layer that is devoted to the implementation of the rules of governance of the platform that are applied to a "Gatekeeper thing" through the release of a certification (Figure 21).

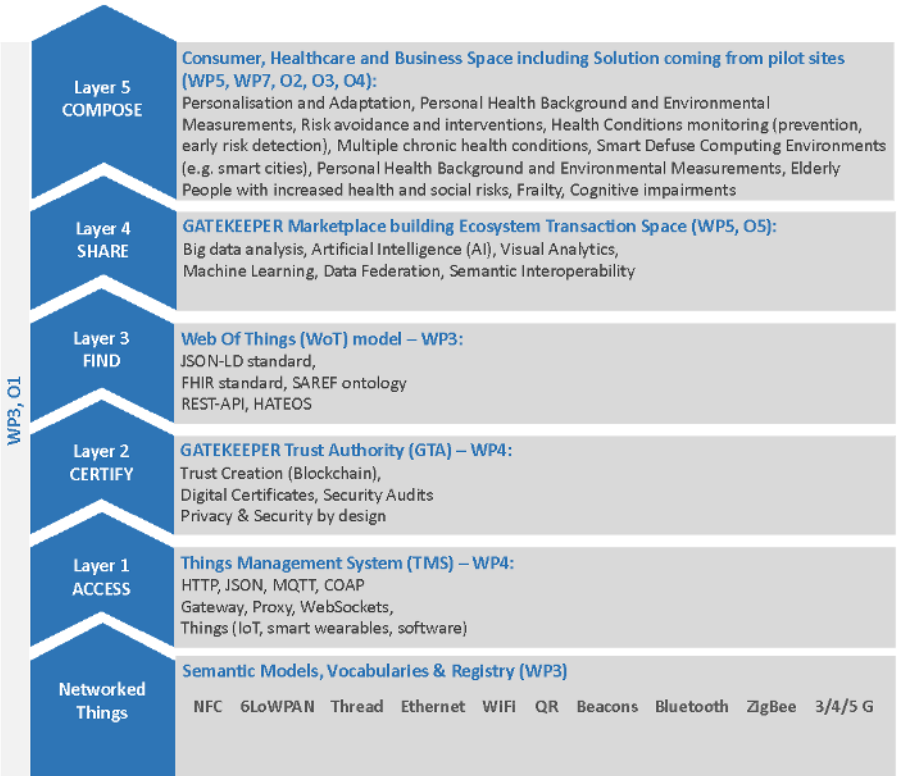

WP3, O1
Layer 5
COMPOSE
Consumer, Healthcare and Business Space including Solution coming from pilot sites (WP5, WP7, O2, O3, O4):
Personalisation and Adaptation, Personal Health Background and Environmental Measurements, Risk avoidance and interventions, Health Conditions monitoring (prevention, early risk detection), Multiple chronic health conditions, Smart Defuse Computing Environments (e.g. smart cities), Personal Health Background and Environmental Measurements, Elderly People with increased health and social risks, Frailty, Cognitive impairments
Layer 4
SHARE
GATEKEEPER Marketplace building Ecosystem Transaction Space (WP5, O5):
Big data analysis, Artificial Intelligence (AI), Visual Analytics,
Machine Learning, Data Federation, Semantic Interoperability
Layer 3
FIND
Web Of Things (WoT) model – WP3:
JSON-LD standard,
FHIR standard, SAREF ontology
REST-API, HATEOS
Layer 2
CERTIFY
GATEKEEPER Trust Authority (GTA) – WP4:
Trust Creation (Blockchain),
Digital Certificates, Security Audits
Privacy & Security by design
Layer 1
ACCESS
Things Management System (TMS) – WP4:
HTTP, JSON, MQTT, COAP
Gateway, Proxy, WebSockets,
Things (IoT, smart wearables, software)
Networked
Things
Semantic Models, Vocabularies & Registry (WP3)
NFC
6LoWPAN
Thread
Ethernet
WIFI
QR
Beacons
Bluetooth
ZigBee
3/4/5 G

Figure 21 - Gatekeeper layered architecture

The different sets of policies are associated with a different kind of certificate, and when a Thing obtains a specific certificate from the Gatekeeper Trust Authority (GTA), it means that this Thing is compliant with the policies associated with the certificate.

Within GTA the policies will be in line to a common set of features that are related with:

- data access compliance with current regulation (e. g. GDPR compliance);

- alignment of data to the Gatekeeper semantic models;
- compliance with standards (mainly Web of Things and FHIR);
- quality of provided data and/or services.

1.1.1 Principles for Gatekeeper data

The main objective behind the data governance inside the Gatekeeper platform is the enhancement of data economy providing solutions for data interoperability and re-use in machine learning (ML) and artificial intelligence (AI) algorithms ensuring data quality, protection, privacy and security.

In order to reach this objective, several principles will be followed for Gatekeeper data:

1. Compliance with Findable, Accessible, Interoperable Reusable (FAIR) principles.
2. Open data as possible, and closed as necessary. Gatekeeper will always provide access to data whenever possible;
3. Clear separation between data owner and data provider. Within Gatekeeper, data will be treated as a Thing (digital twin of the data). So, interfaces in order to access data should be defined as APIs. This means that the data provider should agree with the data owner (e. g. physical database owner) on how and which subset of the data should be made publicly available and/or which kind of restricted access should be implemented.
4. Balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards. These features should be provided by data providers and Gatekeeper will be able to certify its accomplishment through the Certification Authority (GTA).
5. Allow the free flow of non-personal data, Gatekeeper will treat in a high permissive way non-personal and non- sensible data. Less or no certification will be needed in order to include these datasets as Things within the platform.
6. Provide rules for access to and use of data should be fair, practical and clear, with clear and trustworthy data governance mechanisms in place; for an open, but assertive approach to international data flows, data should flow within the EU and across sectors.
7. Allow infrastructures that should support the creation of data pools enabling Big Data analytics and machine learning, in a manner compliant with data protection legislation and competition law, allowing the emergence of data-driven ecosystems.
8. Create an Artificial Intelligence ecosystems based on the concept of Gatekeeper data space that will contribute to the HealthCare Data Space foreseen at European level, with the objective of providing services (WP5) for early prevention and intervention in 7 Medical Reference Use Cases (RUCs defined in WP6) in order to improve the accessibility, effectiveness and sustainability of the healthcare systems.

1.1.2 Gatekeeper Web of Thing based architecture

1.1.2.1 Description of the layered structure

The proposed structure of Gatekeeper Web of Things Platform architecture **Error! Reference source not found.** will be framed into a layered structure composed of: Access, Certify, Find, Share, Compose layers as already shown in Figure 21.

Layer 1: Access, provide Accessibility of FAIR principle: This layer is responsible for turning any Thing into a Web Thing that can be interacted with using HTTP requests just like any other resource on the Web. A Web Thing is a REST API that allows to interact with something in the physical world, like opening a door or reading a sensor located somewhere in the world. In Gatekeeper this layer is provided by the Thing Management System. The Thing Management System (TMS) is one of the core components dedicated to the implementation of the functionality of access and find associated with the access and find layer of WoT architecture. The TMS is like a broker service that publishes the Gatekeeper things, each thing is decorated with a Web of Thing Description that is available through a web based service. Within the TMS, the level of trustiness between the things that are already connected to the platform is automatically managed. The interaction between different things using thing descriptions is defined through an **Web of Things (WoT) interaction model**. The thing description enables: (i) management of multiple Things by a cloud service, (ii) simulation of devices/Things that have not yet been developed, (iii) common applications across devices from different manufacturers that share a common Thing model, (iv) combining multiple models into a Thing. In the next sections, the web of things model will be presented to show the interaction model and architecture of the Web of Things platform.

Layer 2: Certify, improve the FAIR principles with Trustability: This layer is specific to the Gatekeeper platform against the Web of Thing layered reference architecture. It is dedicated to build the concept of trustiness in the Gatekeeper platform through certification and a way to securely share data across services. A Gatekeeper Thing is different against a standard Thing because it has been certified by the Gatekeeper Trust Authority (GTA). Within the Gatekeeper architecture the certify layer is enabled through the interaction between the Things Management System (TMS) and the Gatekeeper Trust Authority (GTA). Gatekeeper Trust Authority will provide the CERTIFY layer of the GATEKEEPER architecture, while the Gatekeeper Marketplace will be in charge of sharing the Gatekeeper things. The Trust creation will be managed using Blockchain with the aim of having a decentralized trust system. As a decentralized system, it removes the requirement for a trusted third party by allowing participants to verify data correctness and ensure its immutability. Things can use blockchains to register themselves and organize, store, and share streams of data effectively and reliably.

Layer 3: Find, provide Findability of FAIR principle: Giving accessibility via HTTP to Things is a good option but it does not mean applications data or services can be easily offered and/or consumed. This layer is dedicated to provide ways for easy discovery and consuming of Things. In Gatekeeper it will be implemented through a Marketplace that will provide things offered through the consumer space, the healthcare space and the business space. Each space is oriented to a different type of market user. These core features will be supported by the Networked things architecture that will provide the reference model in home and health-oriented devices forming the GATEKEEPER Platform's Business Space. The ecosystem will be split into clear boundaries around 3 spaces, Business-to-Government (B2G), Business-to-Consumer (B2C) and Business-to-Business (B2B).

Layer 4: Share, provide Interoperability of FAIR principle: This layer will provide functionalities by which someone can really "understand" what the Thing is, what data or services it offers, and so on. Through these functionalities a Thing can not only be easily used by other HTTP clients but can also be findable and automatically usable by other WoT applications **Error! Reference source not found.Error! Reference source not found.**. The approach here is to reuse web semantic standards to describe things and their services. This enables searching for things through search engines and other web indexes as well as the automatic generation of user interfaces or tools to interact with Things. At this level, technologies such as JSON-LD (a language for semantically annotating JSON) are in use. In Gatekeeper, all the Things will use as communication language the Web of Things standard with JSON-LD contexts, including FHIR standard and SAREF ontology.

Layer 5: Compose, provide Reusability of FAIR principle: This layer provides the integration of data and services from heterogeneous Things into an immense ecosystem of tools such as analytics software, mash-up platforms and developer platforms. Within Gatekeeper the compose layer will provide all the intelligent services for early detection and intervention and a developer platform where developers can compose Gatekeeper things in order to provide advanced services.

All the data pushed from the Things that compounds the ecosystem to the platform will be used by associated with Gatekeeper services, which will aim to create diagnostic and prognostic algorithms, to help not only clinicians and domain experts to support their decisions but also predictive and proactive services to help elderly people at home and in their communities.

In order to build these services, techniques such as big data analysis or artificial intelligence will be of particular importance given the wide range of possibilities they provide. For instance, retrieving multiple datasets from multiple wearable devices could be used to accurately predict possible life threatening diseases such as a stroke or heart attack, thus helping to provide efficient fast assistance.

These early detection, prediction and proactive services for healthcare will be validated in the pilot sites in order to populate the Consumer and Healthcare spaces within the Gatekeeper Marketplace where these services will be available to third party users in order to compose more advanced services through the open calls.

1.1.2.2 Web of Things (WoT) interaction model

Special mention must be given to the Web of Things interaction model which is intimately related to the access layer and the Thing Management System (TMS). The Object model used by the TMS and GTA, and it is composed of three layers: Binding Templates, protocol bindings, and protocol stacks. This model would be an architecture for the interconnection of the different layers of the Web of Things, integrating those Things to the Web and in particular to HTTP, WebSocket, JSON and JSON-LD, using TLS, DTLS, and/or OAuth to authenticate requests. Four main areas are considered inside the Web of things interaction model: Protocols, Resources and Data Model and Semantic Extensions. As seen in Figure 22, the TMS model follows a structured and layered architecture where from the communication protocol, we move onto the TD, then to the contextualized TD and the semantic web distribution.

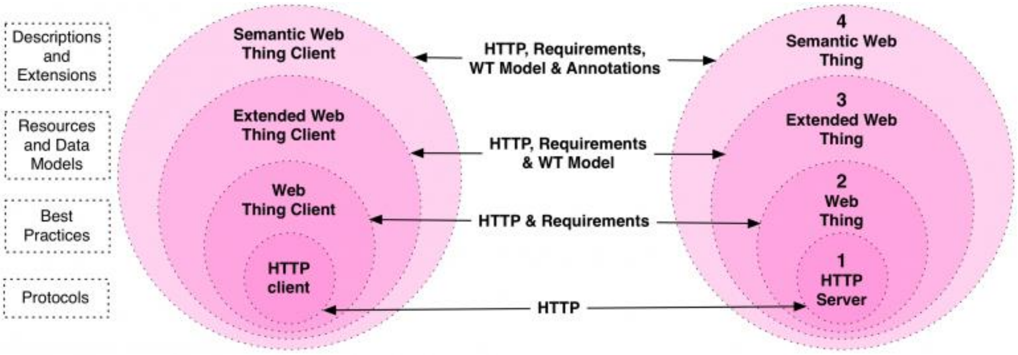

Descriptions and Extensions
Resources and Data Models
Best Practices
Protocols
Semantic Web Thing Client
Extended Web Thing Client
Web Thing Client
HTTP client
HTTP, Requirements, WT Model & Annotations
HTTP, Requirements & WT Model
HTTP & Requirements
HTTP
4 Semantic Web Thing
3 Extended Web Thing
2 Web Thing
1 HTTP Server

Figure 22 - Web of Things model **Error! Reference source not found.**

Binding Templates are a reusable collection of templates used in communication with other platforms. These templates are mapped together with the Protocol Bindings to be used by the Protocol Stack as a guideline for implementation of the web services in HTTP, WebSocket, and CoAP, with JSON and JSON-LD as data-interchange format.

In a large-scale way such as intended with the Gatekeeper Platform, Things pushing data to the web can only happen if the data can be efficiently—and securely—shared across services. This layer specifies how devices and their resources must be secured so that they can only be accessed by authorized users and applications. For that purpose, Things are internally configured in a way that it is divided into different layers with the implementation, definition and communication, through binding templates.

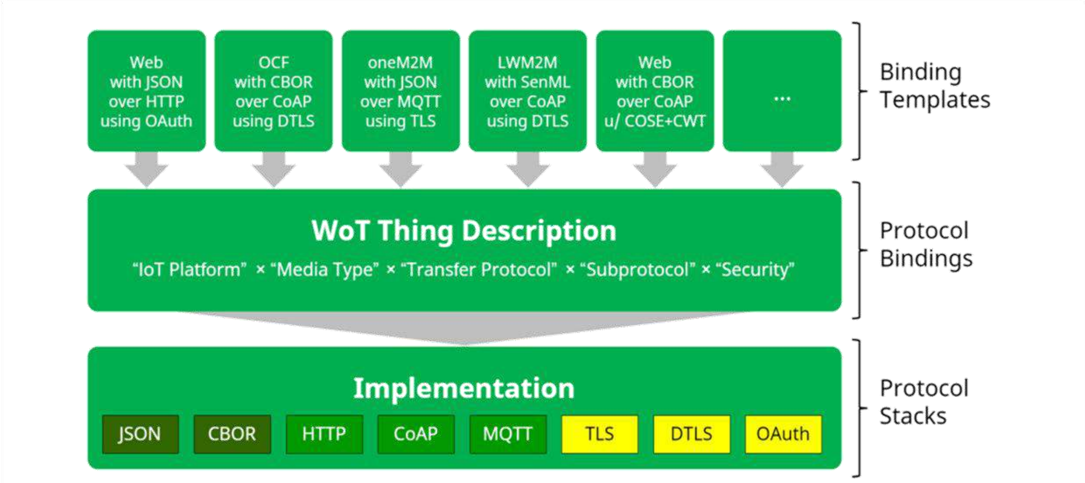

Web with JSON over HTTP using OAuth
OCF with CBOR over CoAP using DTLS
oneM2M with JSON over MQTT using TLS
LWM2M with SenML over CoAP using DTLS
Web with CBOR over CoAP u/ COSE+CWT
...
Binding Templates
WoT Thing Description
"IoT Platform" × "Media Type" × "Transfer Protocol" × "Subprotocol" × "Security"
Protocol Bindings
Implementation
JSON
CBOR
HTTP
CoAP
MQTT
TLS
DTLS
OAuth
Protocol Stacks

Figure 23 - From Binding Templates to Protocol Binding **Error! Reference source not found.**

1.1.3 Role of WoT Thing Description

The Thing Description (TD) is one of the key aspects of the WoT architecture and data models. It allows things to be defined, communicate with each other and expose information. In essence, the web of Thing Description is the entry point of a Thing, and the thing description of the TMS is the point of access to the Gatekeeper ecosystem. It can be understood as the nucleus of the Thing since it provides the functionality of the interconnectivity to the Thing. A thing description consists of four components: (i) *textual metadata about the Thing itself*; (ii) a set of *Interaction Affordances* that indicate how the Thing can be used; (iii) *schemas for the data exchanged* with the Thing for machineunderstandability, and,(iv) *Web links to express any formal or informal relation to other Things or documents* on the Web.

An example of a WoT TD is shown in Example 1. Note that in general, the TD provides metadata for different Protocol Bindings identified by URI schemes and security mechanisms (for authentication, authorization, confidentiality, etc.)

Example 1: Temperature Event with subscription and cancellation. Extracted from **Error! Reference source not found.**

```
{
    "@context": "https://www.w3.org/2019/wot/td/v1",
    "id": "urn:dev:ops:32473-Thing-1234",
    "title": "WebhookThing",
    "description": "Webhook-based Event with subscription and unsubscribe
form.",
    "securityDefinitions": {"nosec_sc": {"scheme": "nosec"}},
    "security": ["nosec_sc"],
    "events": {
        "temperature": {
            "description": "Provides periodic temperature value updates.",
            "subscription": {
                "type": "object",
                "properties": {
                    "callbackURL": {
                        "type": "string",
                        "format": "uri",
                        "description": "unsubscriber for Webhook.",
                        "writeOnly": true
                    },
                    "subscriptionID": {
                        "type": "string",
                        "description": "Unique subscription ID for
cancellation",
                        "readOnly": true
                    }
                }
            },
            "data": {
                "type": "number",
                "description": "Latest temperature value"
            },
            "cancellation": {
                "type": "object",
                "properties": {
                    "subscriptionID": {
                        "type": "integer",
                        "description": "Required to cancel subscription.",
                        "writeOnly": true
                    }
                }
            },
            "uriVariables": {
                "subscriptionID": { "type": "string" }
            },
            "forms": [
                {
                    "op": "subscribeevent",
                    "href":
"http://192.168.0.124:8080/events/temp/subscribe",
                    "contentType": "application/json",
                    "htv:methodName": "POST"
                },
                {
                    "op": "unsubscribeevent",
                    "href":
"http://192.168.0.124:8080/events/temp/{subID}",
                    "htv:methodName": "DELETE"
                }
            ]
        }
    }
}
```

In Example 1, a Thing Description is shown to represent a Webhook event. The context definition in this case has included HTTP protocol bindings supplements. The TD doesn't have security as defined in "securityDefinitions" and "security" fields. The TD provides an Event affordance called "temperature" that updates its latest temperature value to the consumer. It sends a POST request to a callback URI that is provided by the consumer. The "subscription" defines two properties, one is a write-only parameter called "callbackURL" that must be submitted through the subscribeevent. The other property, "subscriptionID" is read-only and returned by the subscription. In case of subscription the Thing would send periodically its state through a POST to the callback URI using "data" form defined structure. To unsubscribe, the "unsubscribeevent" form must be submitted, this form makes use of a URI Template to specify the subscription to cancel. The uriVariables member functions as a note to the consumer to include its contents. Alternatively, the member "cancellation" can be used to unsubscribe in a similar way to "subscription" and combine it with a subscribeevent form.

For the Thing Description the use of JSON-LD is crucial as it is a lightweight Linked Data format for linking data with vocabularies that describe the semantic of the data. Another important aspect of the JSON-LD data format is its human readability. It is based on the already existing JSON format and provides a way to help JSON data interoperate at Web-scale through the concept of context. JSON-LD is an ideal data format for programming environments, REST Web services, and unstructured databases such as CouchDB and MongoDB, although it also gives very useful functionalities to Web of Things. A simple example of a JSON-LD is shown in Example 2. The use of the contexts allows JSON-LD to map data.

Example 2: Example of a JSON-LD. Extracted from **Error! Reference source not found.**

```
{
  "@context": "https://json-ld.org/contexts/person.jsonld",
  "@id": "http://dbpedia.org/resource/John_Lennon",
  "name": "John Lennon",
  "born": "1940-10-09",
  "spouse": "http://dbpedia.org/resource/Cynthia_Lennon"
}
```

Example 2 shows a simple JSON-LD where the context links the data structure of the JSON with the concept of Person of the ontology friend of a friend (FoaF) described in the

URI https://json-ld.org/contexts/person.jsonld. Based on such context the terms "Name", "born" and "spouse" have a clear semantic meaning and can be understood by machine and humans.

The vocabulary of the Thing description is divided into: core, data schema, WoT security and Hypermedia Controls vocabularies. The interaction models between things, conceptual basis of the processing of thing descriptions and their serialization.

The Thing Description information **Error! Reference source not found.** model is built in:

- Core vocabulary, which reflects the Interaction Model with the Properties, Actions, and Events Interaction Affordances.
- Data Schema vocabulary, including (a subset of) the terms defined by JSON Schema.
- WoT Security vocabulary, identifying security mechanisms and requirements for their configuration.

Hypermedia Controls vocabulary, encoding the main principles of RESTful communication using Web links and forms.

The vocabularies introduced before are the main parts of the TD information model, then, the elements that put together all the things, i.e. platforms, wearables, web services. Therefore, they must be understood in order to create a framework based on this paradigm.

A Thing defined as a Thing Description includes the following properties fields: context, type, id, title, description, properties, actions, events, forms, security and security definitions, among others. In Table 17, a compilation of all the fields that are included in the Thing Description is shown.

Table 17: Core vocabulary of Thing Description **Error! Reference source not found.**

Vocabulary term	Description	Assignment	Type
@context	JSON-LD keyword to define short-hand names called terms that are used throughout a TD document.	mandatory	anyURI or Array
@type	JSON-LD keyword to label the object with semantic tags (or types).	optional	string
id	Identifier of the Thing in form of a URI RFC3986[11] (e.g., stable URI, temporary and mutable URI, URI with local IP address, URN, etc.).	optional	anyURI

[11] Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee; R. Fielding; L. Masinter. IETF. January 2005. Internet Standard. URL: https://tools.ietf.org/html/rfc3986

Vocabulary term	Description	Assignment	Type
title	Provides a human-readable title (e.g., display a text for UI representation) based on a default language.	mandatory	String
titles	Provides multi-language human-readable titles (e.g., display a text for UI representation in different languages).	optional	MultiLanguage
description	Provides additional (human-readable) information based on a default language.	optional	string
descriptions	Can be used to support (human-readable) information in different languages.	optional	MultiLanguage
version	Provides version information.	optional	VersionInfo
created	Provides information when the TD instance was created.	optional	dateTime
modified	Provides information when the TD instance was last modified.	optional	dateTime
support	Provides information about the TD maintainer as URI scheme (e.g., mailto RFC6068[12], tel RFC3966[13], https).	optional	anyURI
base	Define the base URI that is used for all relative URI references throughout a TD document. In TD instances, all relative URIs are resolved relative to the base URI using the algorithm defined in RFC3986. base does not affect the URIs used in @context and the IRIs used within Linked Data[14] graphs that are relevant when semantic processing is applied to TD instances.	optional	anyURI
properties	All Property-based Interaction Affordances of the Thing.	optional	Map of PropertyAffordance
actions	All Action-based Interaction Affordances of the Thing.	optional	Map of ActionAffordance
events	All Event-based Interaction Affordances of the Thing.	optional	Map of EventAffordance

[12] The 'mailto' URI Scheme. M. Duerst; L. Masinter; J. Zawinski. IETF. October 2010. Proposed Standard. URL: https://tools.ietf.org/html/rfc6068

[13] The tel URI for Telephone Numbers. H. Schulzrinne. IETF. December 2004. Proposed Standard. URL: https://tools.ietf.org/html/rfc3966

[14] Linked Data Design Issues. Tim Berners-Lee. W3C. 27 July 2006. W3C-Internal Document. URL: https://www.w3.org/DesignIssues/LinkedData.html

Vocabulary term	Description	Assignment	Type
links	Provides Web links to arbitrary resources that relate to the specified Thing Description.	optional	Array of Link
forms	Set of form hypermedia controls that describe how an operation can be performed. Forms are serializations of Protocol Bindings. In this version of TD, all operations that can be described at the Thing level are concerning how to interact with the Thing's Properties collectively at once.	optional	Array of Form
security	Set of security definition names, chosen from those defined in securityDefinitions. These must all be satisfied for access to resources.	mandatory	string or Array of string
securityDefinitions	Set of named security configurations (definitions only). Not actually applied unless names are used in a security name-value pair.	mandatory	Map of SecurityScheme

The Thing Description offers the possibility to add contextual definitions in some namespace. This mechanism can be used to integrate additional semantics to the content of the Thing Description instance, provided that formal knowledge, e.g., logic rules for a specific domain of application, can be found under the given namespace. The contextual information also specifies some configurations and behaviour of the underlying communication protocols declared in the forms field.

Web of Things use of Thing Description is similar to OpenAPI although there are important differences.

- In terms of security, while the HTTP security schemes, Vocabulary, and syntax given in this specification share many similarities with OpenAPI, they are not compatible, making this a big challenge for harmonizing OpenAPI with Web of Thing.
- While OpenAPI is an open specification standard for exposing an API with a set of rules, the thing description is a standard that is more general it allows to expose a thing, being understood as a device, service, platform or whatever.
- OpenAPI does not support semantic annotation while Web of Thing description is allowing the inclusion of contexts with JSON-LD that are used for describing the semantic of the data within the Thing Description.

1.1.4 Role of FHIR and relation with Thing Description

FHIR will be a core concept within Gatekeeper. It is a very mature standard provided by HL7, commonly used in the healthcare domain around the world with a wide community of developers and adopters. Details on FHIR will be provided in the D3.4 and D3.5 but for understanding how it will be used within Gatekeeper some basic notions will be provided.

FHIR is a REST-ful based approach for modelling data structures as Healthcare Resources and services as REST-APIs in order to provide a solution for health interoperability. Furthermore, it addresses the semantic health interoperability between healthcare centre providing a dynamic standardized approach for the definition of the terminology used within a healthcare centre. In a very smart way it is solving semantic interoperability between different healthcare centres standardizing the rules that allow terminology inconsistency between them. When an adopter would use FHIR it should define a FHIR Profile Resource where is defined the health terminology (e. g. SNOMED-CT, ICD, LOINC, etc.) used by the adopter. In this way 2 different adopters will differ at semantical level only in the definition of their profiles and interoperability could be reached by mapping of the terminologies used in their Profile Resources. The definition of a FHIR implementation guide and Gatekeeper FHIR profiles will be the based for the Gatekeeper healthcare data space.

Apart of Profile resources, FHIR also provides Conformance Resource. This resource is a description of the services (signatures, profiles, data exchanged, allowed parameters, etc..) provided by each endpoint of the FHIR implementation.

In the context of Gatekeeper, a FHIR Conformance Resource is the same of a Things Description because it is describing the whole set of services included within the FHIR implementation. So, we need to avoid an unnecessary overwriting of functionalities and find a way that Thing Description and FHIR conformance resource can coexist within the platform. In this case the solution for the integration of both approaches is to integrate a FHIR Conformance Resource within a Thing Description by linking the endpoint that is providing the Conformance Resources as showed in the following example:

Example 3: FHIR Conformance Resource in the Thing Descriptor

```
{
  "@context": [
    "https://www.w3.org/2019/wot/td/v1",
    {
      "xsd": "http://www.w3.org/2001/XMLSchema#",
      "FHIRServer":  {"@id": "td:Thing"},
      "conformance": {"@id": "xsd:anyURI"}
    }
  ],
  "@type":"FHIRServer",
  "title": "Gatekeeper pilot x FHIR server",
  "description" : "A FHIR server implementation",
  "securityDefinitions": {
    "no_sec": {
      "scheme": "nosec"
    }
  },
  "security": [
      "no_sec"
  ],
  "conformance": "http://hapi.fhir.org/conformance?serverId=home_r4"
}
```

1.2 Gatekeeper Platform Stakeholders

Stakeholders that are interested in the results of the Gatekeeper project can be differentiated of two types: the platform stakeholders, who interact and use the software, and project stakeholders, who are the ones who do not interact directly with the solution but are somehow affected by it.

This deliverable tries to combine the analysis of D2.3 and the domain knowledge expressed in D6.2, with a specific focus on platform stakeholders to identify them and the role they cover in the usage of the platform.

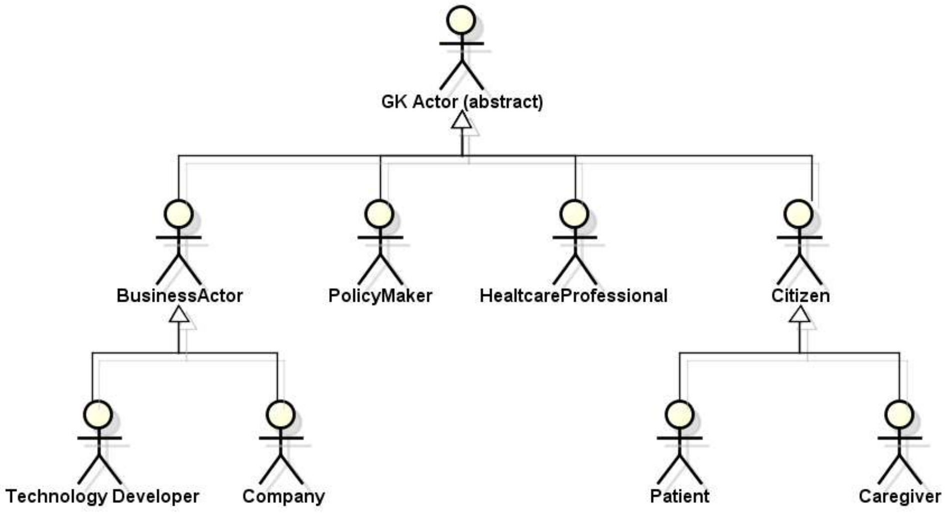


Figure 24 - Gatekeeper platform stakeholders

BUSINESS ACTOR

Extends: GK Actor (Abstract)

Description: Generic stakeholder of the Business space. He/she is the provider of marketable solutions that integrate with the GK platform

Concrete Implementers: Medtech Companies, Developers, IoT or HC Device providers

TECHNOLOGY DEVELOPER

Extends: Business Actor

Description: Develops solutions that exploit the existing Gatekeeper services

Concrete Implementers: Solution developer

COMPANY

Extends: Business Actor

Description: Produces and markets health and wellbeing KETs

Concrete Implementers:

POLICY MAKER

Extends: GK Actor (Abstract)

Description: Administrator of the GK Platform. Manages the governance policies of the regulating the platform

Concrete Implementers: Governments, HC Systems

HEALTHCARE PROFESSIONAL

Extends: GK Actor (Abstract)

Description: A Professional Caregiver is a person who provide care to those who need supervision or assistance in illness or disability. They use Gatekeeper technology and solutions to assist person or citizen

Concrete Implementers: General Practitioner, Nurse, Pharmacist

CITIZEN

Extends: GK Actor (Abstract)

Description: Citizen represents people who might be interested in the results of GATEKEEPER Interventions, directly (in the case of patients) or indirectly (for Caregivers). They consume health services.

Concrete Implementers: Patients, Informal caregivers

PATIENT

Extends: Citizen

Description: A Patient is a person receiving or registered to receive medical treatment. He/she is the owner of personal health and wellbeing data

Concrete Implementers: Elderly Citizen, Patients with co-morbidities.

CAREGIVER

Extends: Citizen

Description: Provides formal or informal care to one or more Elderly Citizens

Concrete Implementers: Assistant, Social Worker, Family Memeber

1.3 Security and Privacy considerations

The conceptual approach of the Security and Privacy module of GK follows the principles of the Reference Model of International Data Space Association. The trustworthy Architecture focuses on exploiting and sharing things from various sources in any type of scenarios, including cross-border cases. The Security and Privacy framework leverages existing standards, technologies and established governance models, to facilitate secure and standardized data exchange and data linkage in trusted ecosystems.

In detail, security and privacy considerations will be ensured by five main architectural elements: a) the User management, b) the Certification Authority, c) the Dynamic Attribute Provisioning, d) the Thing Action Tracking / Audit and e) the Clearing House (exposed as Thing).

The Certification Authority (CA) is responsible for issuing, validating and revoking digital certificates. A digital certificate is provided for a user and a thing based on the validation mechanism. The Validation is implemented based on standardisation methods that will be delivered by T8.1.

The Dynamic Attribute Provisioning Service (DAPS) includes master data and information on security profiles. Since the CA provides the details on the digital certificate, the participant registers at the DAPS. Then the User Management mechanism identifies the validated users and gives permissions for the trusted to access the GK platform. Furthermore, the validated things are delivered to the TMS system. DAPS is also responsible for the management of dynamic consents and FAIRification Principles of Things.

Dynamic Trust Monitoring (DTM) is necessary for classification of the trustworthiness of all participants in the ecosystem. DTM implements a monitoring function for everything and shares information with the DAPS to notify on the trustworthiness of the transactions. Furthermore trails of all transactions related to things, maintaining a detailed history of the whole thing lifecycle.

The Clearing House logs all activities performed in the course of a data exchange. After a data exchange, or parts of it, has been completed, both the Data Provider and the Data Consumer confirm the data transfer by logging the details of the transaction at the Clearing House. The logging information can also be used to resolve conflicts. The Clearing House also provides reports on the performed (logged) transactions for billing, conflict resolution, etc. This task is responsible for the adoption of FAIRification principles after a thing is consumed. Thus the Clearing House will be also exposed as a thing and delivered to the end-users of the GK platform.

1.3.1 Infrastructure security

In order to address security and privacy issues, the Gatekeeper Data Centre infrastructure managed by HPE uses a number of technologies, products and services:

- VPN access, by means of OpenVPN open source software. Two kinds of VPN profiles are available:
  - *Road warrior,* for Gatekeeper partners users, supporting on-demand connections from PC clients
  - *Site-to-site,* for Gatekeeper pilots, supporting always-on connections from Pilot sites
- Support for different VPN access authentication types:
  - *Single Factor (user and password)*
  - *Two Factor Authentication (2FA)*
  - *Multi Factor Authentication (Client Certificate + Password + OTP)*
- Firewall devices and policies. They are used to determine whether a given user/pilot can access a network or a Gatekeeper service
- Security services. They are managed by HPE and include:
  - Identity Management: user identities to access services (e.g. VPN, servers, VMs) are centrally managed by HPE
  - Public Key Infrastructure (PKI): HPE manages an internal private Certification Authority that releases digital certificates (e.g. for VPN user access or internal web sites/services) and manages their lifecycle (e.g. revocation)
  - Intrusion Detection System (IDS): a service to block malicious attacks based on security rulesets
  - Proxy Server: access to the Internet from HPE Data Centre is controlled and filtered via an HTTP Proxy Server
  - Log Management: all devices (e.g. operating system, backup, switches, firewalls, etc.) are traced, and logs are kept in a Log Management system for security purposes

2 GATEKEEPER Architecture

2.1 Logical Architecture

This section highlights the context and role of GateKeeper platform by giving an overview of the platform as a whole and the roles of the single components.

The following figures highlight the context of the Gatekeeper platform by means of functionals views. Components colors highlight their role. Pink components represent Core Pltform Things (from WP4), blue components are Integrated Dynamic intervention Things (WP5), while yellow components represent External things that can interact with the platform and respond to sepcific needs of Pilots or in general respond to specific application requirements. The solid arrows demonstrate the main flows of the significant data managed by the Platform.

The dashed arrows in the figues demonstrate the significant interactions of stakeholders that trigger the main data flows. For clarity, we split such flows to hilight the ones that concern the Business and Transactions spaces and the ones that emerge from the use in the Consumer and Healthcare spaces. A detailed description of the actors involved can be found in Section 1.2. The role of the Platform components is described in more details below, but the flows can be summarized in the following coarse grained sequences:

1. The Policy Maker manages the platform by moterating the MarketService content and managing the security and privacy policies in the Trust Authority (Transaction space)
2. Developers integrate the Platform serivices in customer solutions or develop new Things to be integrated in the platform. Business actors (Developers, but also Companies) publish new offerings of Things in the Marketplace, (Business space)
3. Sensor data produced along the execution of activities/exercises by the patient are fed (collected in connectors or directly) to the platform together with data from EHRs. Data are federated in the platform and processed by Dynamic Intervention services. Data and results are visualized by Healthcare professionals and Patients using the registered applications (Consumer and Healthcare spaces).

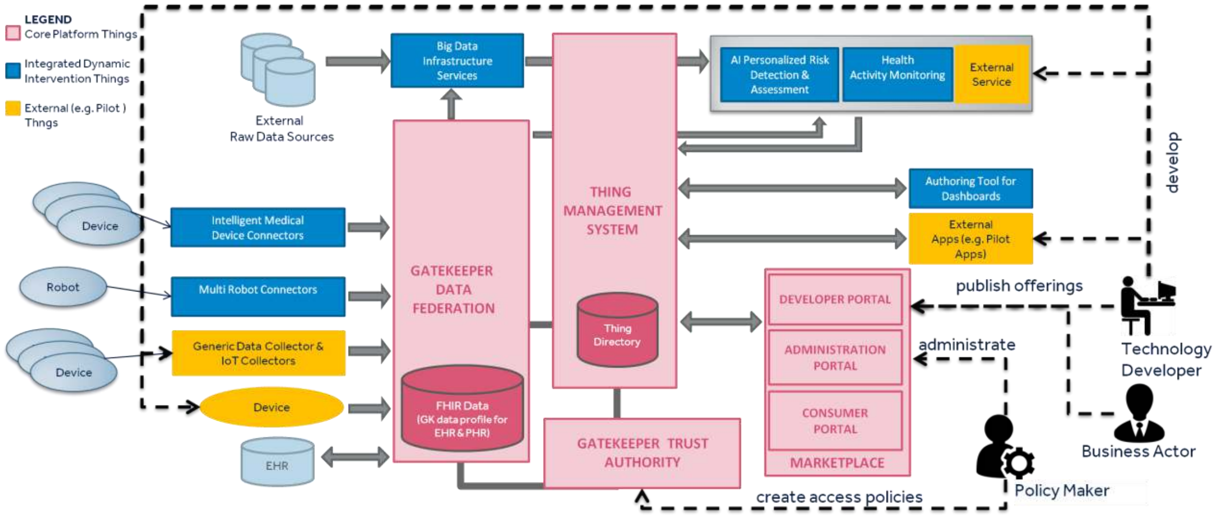

LEGEND
Core Platform Things
Integrated Dynamic Intervention Things
External (e.g. Pilot) Thngs
External Raw Data Sources
Big Data Infrastructure Services
THING MANAGEMENT SYSTEM
AI Personalized Risk Detection & Assessment
Health Activity Monitoring
External Service
develop
Authoring Tool for Dashboards
External Apps (e.g. Pilot Apps)
Device
Intelligent Medical Device Connectors
Robot
Multi Robot Connectors
Device
Generic Data Collector & IoT Collectors
Device
EHR
GATEKEEPER DATA FEDERATION
FHIR Data (GK data profile for EHR & PHR)
Thing Directory
GATEKEEPER TRUST AUTHORITY
DEVELOPER PORTAL
ADMINISTRATION PORTAL
CONSUMER PORTAL
MARKETPLACE
publish offerings
administrate
Technology Developer
Business Actor
Policy Maker
create access policies

Figure 25 –Gatekeeper Architecture view - Business and Transaction spaces

In all contexts of usage the **Things Management System** functions as the entry point of the GateKeeper platform. It manages Things (devices, services, platform or other assets to be operated as an individual elements) represented as Thing Descriptors, following the Web Of Things approach (Section 1.1). It keeps a registry of such Things in the Thing Directory and also acts as an API Gateway mediating any interaction between Things and their consumers using the policies set by the Trust Authority.

Such policies and usage rights are managed by the *Policy Maker*, who administers the Platform ensuring laws and regulations are enforced by such policies, and supervises registered users and things.

The **Trust Authority** is the component that is responsible to enforce such policies and act as a Certification Authority for Things. It applies certification tests to the Things ensuring that a thing respects the rules of the different GateKeeper Thing profiles (medical device certification, interoperability with standards, GDPR compliance, etc). The Trust Authority also checks authorization rights for the access to services and data throughout the platform.

The **GateKeeper Marketplace** is the single-entry point for all users to explore, conceptualize, test and consume the added value services they are interested in. It will allow a uniform access to the Things ecosystems and will acheive interoperability by enabling service/application exchange between deployment sites, third-parties, etc. For developers in particular, it will provide a **Developer Portal** allowing to find development and deployment material in order to publish applications and services. It will also deploy applications/services to the cloud or on premise at ease.

Developers will be also supported by the **Authoring Tool** to build and integrate UI easily in their solutions.

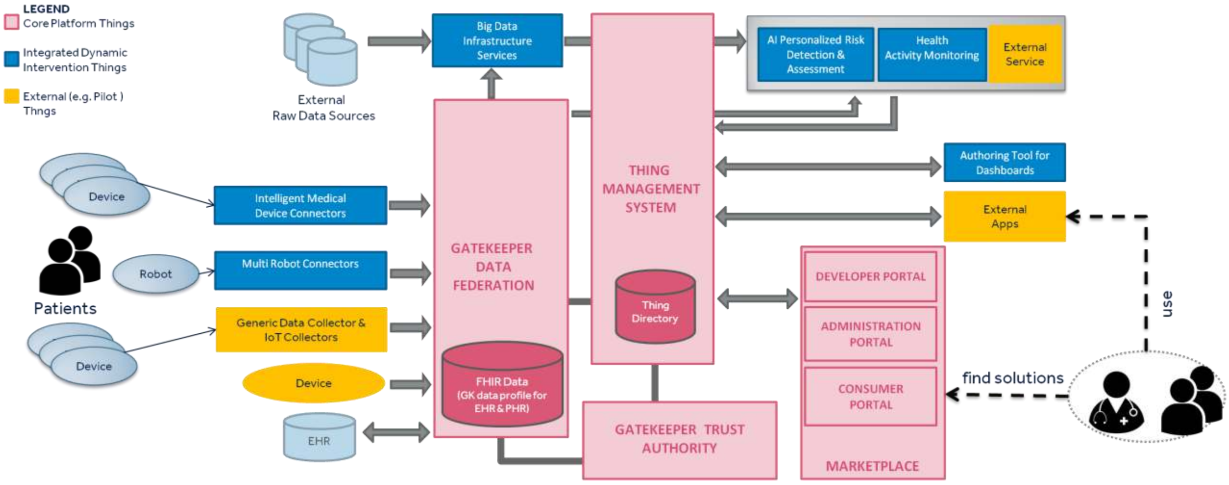

LEGEND
Core Platform Things
Integrated Dynamic Intervention Things
External (e.g. Pilot) Thngs
External Raw Data Sources
Big Data Infrastructure Services
AI Personalized Risk Detection & Assessment
Health Activity Monitoring
External Service
Device
Patients
Robot
Device
Intelligent Medical Device Connectors
Multi Robot Connectors
Generic Data Collector & IoT Collectors
Device
EHR
GATEKEEPER DATA FEDERATION
FHIR Data (GK data profile for EHR & PHR)
THING MANAGEMENT SYSTEM
Thing Directory
GATEKEEPER TRUST AUTHORITY
Authoring Tool for Dashboards
External Apps
DEVELOPER PORTAL
ADMINISTRATION PORTAL
CONSUMER PORTAL
MARKETPLACE
use
find solutions

Figure 26 –Gatekeeper Architecture view – Consumer and Healthcare spaces

Health and environmental data that are processed by platform can come from data connectors or devices provided by pilots or companies and are registered and certified in the platform as Things, or even directly accessed from EHRs. GateKeeper Platform already provides two types of connectors:

The **Intelligent Medical Device Connector**, that allows to access device measurement data regardless of their differences in inferfaces or connection protocols, and homogenize their data format; the **Multi robot connector**, the connector that allows to interact and get information from robots.

GateKeeper Data Federation service is responsible to integrate and federate data coming from the different sources. It provides a set of southbound interfaces to connect to the different data providers. Data can be sent explicitly by the connectors and devices exploiting the provided rest interface or be configured to periodically read data from EHR or other data sources.

Using semantic models, data are transformed in a unique format, the GateKeeper FHIR Data Profile, and made available to the rest of the GateKeeper Platform and all Things authorized to access them.

Data integrated in the data federation are also pushed to the **Big Data Infrastructure**, where they can further processed and merged with external data sources.

The infrastructure will provide services to preform Big Data analysis and generic models that can be exploited from the other services registered in the platform as Things.

In the plaform will be also available two processing services: the **AI Personalized Risk Detection & Assessment**, that will provide diagnostic and prognostic algorithms that can help both professionals to support their decisions and elderly with no technical knowledge to improve their independency and ability over the time; **Home and Health Activity Monitoring** that can combine Personal Health Background and Environmental Measurements, mapping of daily activities and environmental threats at home, to identify and notify abnormal conditions.

Following figure 16 shows the UML domain model associated to the Gatekeeper platform.

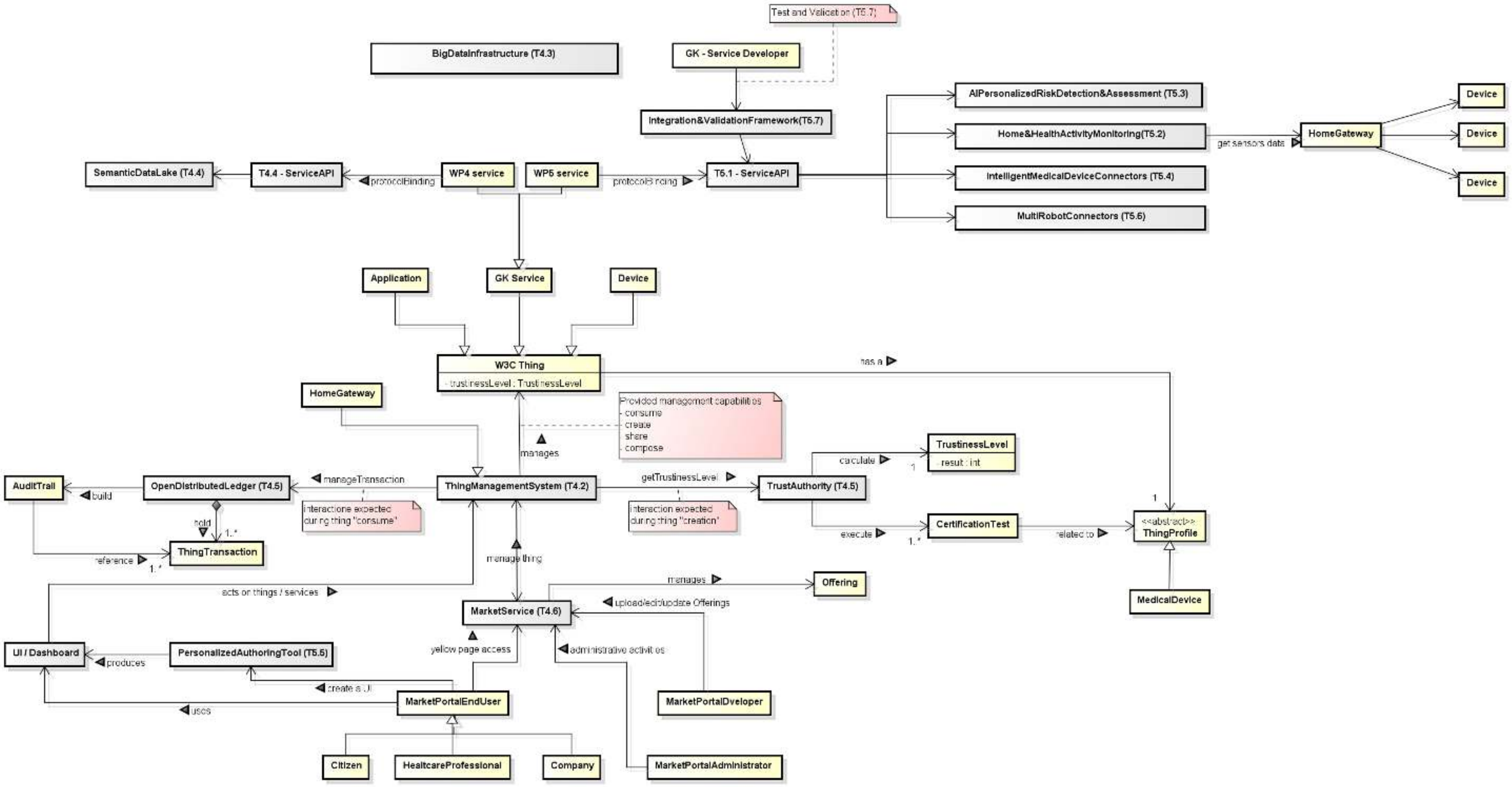


Figure 27 - High level UML Domain Model

3 Information Model

The Information Model shown in the diagrams below describes the main types of data exchanged between the Gatekeeper components.

The Information Model described focuses on two aspects: entities, and their relationships, directly used as input and output parameters of the operations provided by components (listed in section **4**); an initial entity diagram that represents the Health related measurements used by pilots, as gathered by the analysis of D6.2, that will be the basis of the work of tasks 3.4 and 3.5 for the creation and formalization of a unified Gatekeeper semantic model.

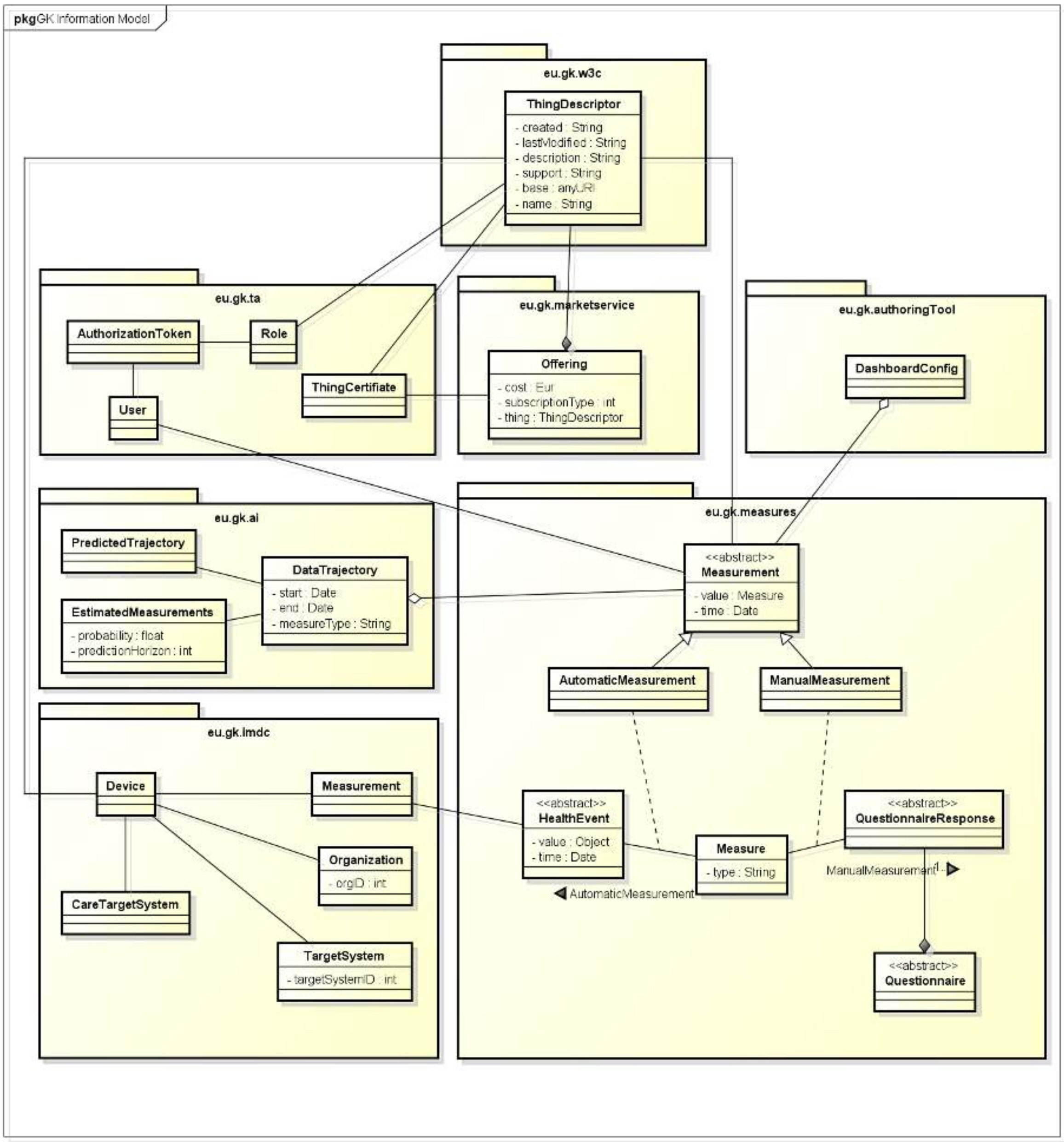


Figure 28 - Gatekeeper Information Model

The reported Information Model (Figure 28) focuses on data involved in the component interactions defined so far in the project. The model will be continuously enriched with new entities, when the interfaces of the components will be further defined.

The main data type for this platform is the *ThingDescriptor* described in detail in section 1.1.3. It contains descriptions of all services and things (sensors, *Devices*) that by invoking their actions can produce or elaborate health data (*Measurements*) in the platform.

To regulate the access to the ThingDescriptor, and perform actions, the Trust Authority links to the TD a set or authorized *Roles.* Roles are assigned to registered *Users* and they obtain *AuthorizationTokens* to prove their identities.

A thing is referred in the MarketService by means of the *Offering* entity. This entity is the representation of all added value services exposed by the Gatekeeper Platform. When an Offering describes a software service or device that can be connected to the GK platform, it links to its *ThingDescriptor*.

The *IntelligentMedicalDeviceConnectors* thing can manage *Devices*, representing sensors that generate *Measurements* of patients status. Devices belong to *Organizations*. Devices and their measurements can be accessed by *Users* with different *Roles.*

Measurements represent the Health data managed by the platform. They refer to *Measure* types, of a variety of health related aspects. An initial set of Measures obtained by the analysis of Pilots is detailed in the next section.

All Measurements the platform manages are collected from connectors in a variety of formats (the task dealing with the identification of such formats is T3.4) and being translated in a homogeneous format to federate them and allow a homogeneous access. The target format will be formalized in the Gatekeeper FHIR profile, output of T3.5.

Federated data can be visualized using the services of the AuthoringTool that uses *DashboardConfigs* to customize views on the *Measurements*.

Data are also processed by Dynamic Intervention services that take as input *DataTrajectories* and by the use of AI algorithms can produce Risk assessments or *Predicted Trajectories*. Details on the input and output requirements for such services is detailed in section **Error! Reference source not found.**.

3.1 Health Measures

Although details on the work of mapping input measures and their formats from pilots and defining a unique Gatekeeper FHIR profile that is able to represent them is a joint work of T3.4 (for the concepts identification and mapping) and T3.5 (for the definition of the FHIR profile), here we give an initial overview of health measure types that the platform will manage.

Figure 29 show the result of the analysis of the list of measures required by pilots as reported in D6.2. *Measures* that the Gatekeeper platform will have to manage comprehend *Vital Signs* (such as *Body Temperature*, *ECG*, *Respiratory Rate*), as well as data on the patient *Activity* or other parameters as *Glucose* or Sweat level.

A specific value in time of a Measure is captured by the *Measurement* entity, that describes a Measure, its value, the patient identifier and the time it was captured.

Measurements are first categorized based on the way they are captured. They can be *AuomaticMearurements*, produced by *HealthEvents*, or *ManualMeasurements* coming from the *QuestionnaireResponses* of *Questionnaires* of self assessment or interviews with professionals.

HealthEvents can be generated from Devices or be the result of the data processing of Dynamic Intervention Services. In the latter case they are referred as *Risk Events*.

Questionnaires can cover a variety of topics, from *Helthy Habits*, to *Cognitive Impairment*, *Dependencies*, *Medications* or *Emotional Situation*.

3.1.1 Gatekeeper FHIR profile

A FHIR profile is a set of rules which allows a FHIR resource to be constrained or include extensions so it can add additional attributes. T3,5 will take as input all the information on relevant Resources to be included in the profile (output of T3.4), and formalize a Gatekeeper FHIR profile to ensure data will be semantically interoperable. The profile will be based on v4 of FHIR **Error! Reference source not found.**.

The translation from the original format to the GK FHIR profile will be performed by the Gatekeeper federation component, that will also provide a FHIRv4 compliant database to store the translated data and make them available for the rest of the platform.

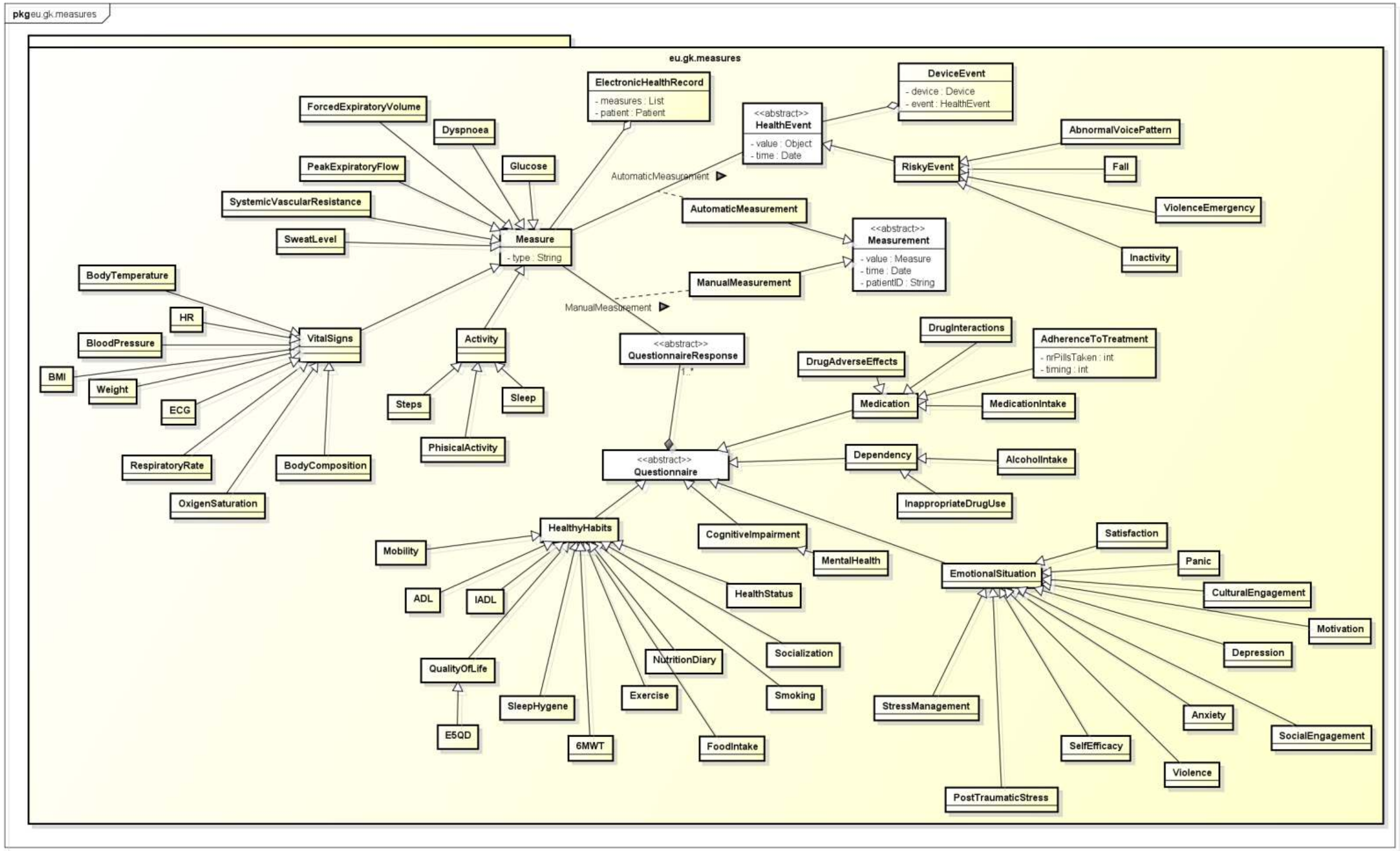


Figure 29 - GK Health Information Model

4 GateKeeper Components

In this document the components reported below are considered as black-box and, as such, no information is reported about their internal architecture which is documented in other deliverables. The following table provides a guide of the context where these components are provided and thus documented.

Table 18: Components list overview

Component Name	Responsible	Task
Things Management System	UPM	4.2
Things Directory	UPM	4.2
Error! Reference source not found.	HPE	4.3
GK-IntegrationEngine	ENG	4.4
GK-FHIRServer	ENG	4.4
RDF Semantic Data Lake	ENG	4.4
Trust Authority	CERTH	4.5
Error! Reference source not found.	CERTH	4.6
Error! Reference source not found.	SAMSUNG	5.2
Error! Reference source not found.	MYS	5.3
Error! Reference source not found.	MEDISANTE	5.4
Error! Reference source not found.	TECNALIA	5.5
Error! Reference source not found.	OU	5.6

For the first release of the platform only components highlighted in gray in table 2 will be provided.

4.1 Things Management System

The Things Management System (TMS) is the entry point of the GateKeeper platform. In analogy to a classical microservices architecture it is like an API gateway component.

The TMS will not manage directly REST-API like a common API Gateway but it will manage Things represented as Thing Descriptor. A representation of this functionality is shown in Figure 30, and it is based on the intermediary architecture described in the Web of Things architecture specifications (https://www.w3.org/TR/wot-architecture/).

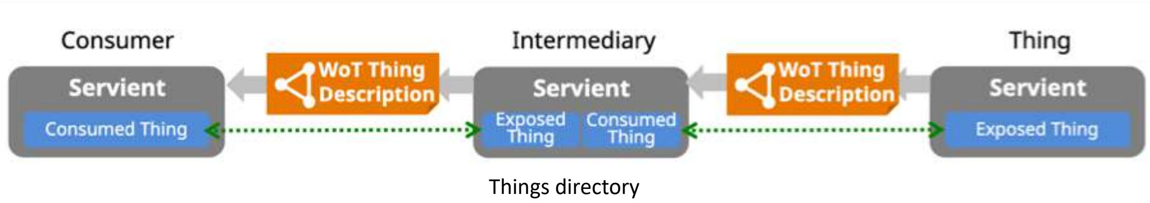


Figure 30 - Conceptual Diagram of the GateKeeper Thing Management System (TMS).

The Thing Management System is the intermediate in any interaction between things and consumers. We define thing as any device, service or platform that is standardize with a model of data to be operated as an individual element derived from a set of predefined templates like smart light-bulbs, smartwatches, AI service or marketplace analytics platform. In Figure 31 it can be seen the inner architecture of Thing Management System and its components.

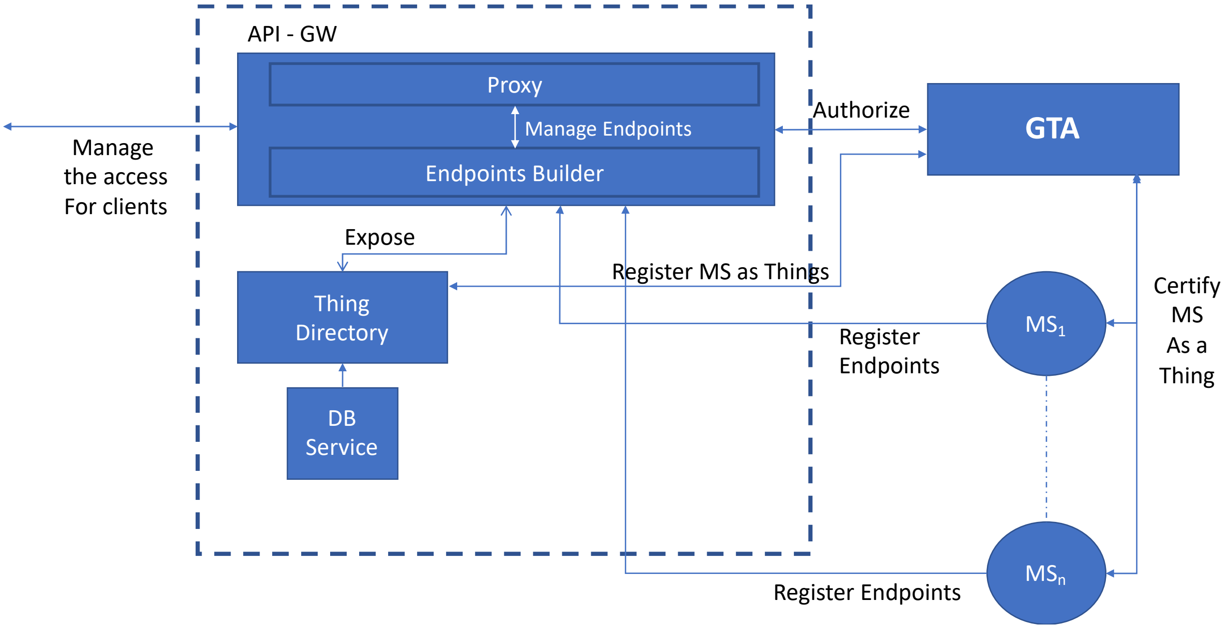


Figure 31 - GateKeeper Thing Management System (TMS) inner architecture.

In the architecture of the GateKeeper Thing Management System, it can be identified the following components:

- GTA: GateKeeper Trust Authority (T4.5), it manages authentication and authorization of users in order to consume things
- Thing Descriptor (TD) – descriptor of the thing compliant with WoT object model and GK semantics (T3.3, T3.4).
- API - GW – Gateway for RESTful interfaces (or other protocols) of GK services
  - Proxy: Redirect requests to different microservices (only for REST interfaces)
  - Builder: Interact with GTA for building and register new endpoints

- Thing Directory TMS – TD – Directory that collect all GK Things
  - It's the WoT Runtime (e. g. ArenaWebHub) It should provide access to standardized URL for properties, actions, events like Mozilla does
- MSx: Microservice x providing service x as REST API

Two use cases have been described for the analysis of the components and functionalities that must be considered for the definition of the interfaces: (i) first use of a thing and (ii) normal use of the thing.

The first use case, which is shown in **Error! Reference source not found.**, represents the interaction between the user and the platform for the first time that the thing is used. Since in the first use case it is needed to ask for an authorization and certify the component. In the second use case (**Error! Reference source not found.**), the component is already recognizable by the GateKeeper Trust Authority and used directly thought the right permission.

ThingManagementService Provided Interface		
access() : anyURI		
Ask to the TMS for the access to the thing.		
Input(s)	--	
Output	thing:anyURI	*Thing Descriptor of the TMS with security definition (e. g. Bearer authentication)*
registerForUser(String): anyURI		
Register a Things for the user		
Input(s)	thing:String	*The serialized Thing (see section* 1.1.3*) to register*
Output	thing:anyURI	*Thing Descriptor of the TMS with security definition (e. g. Bearer authentication)*
getTMSDescriptor(String): anyURI		
Ask to the TMS for the Thing Descriptor		
Input(s)	thingDescriptor: String	*The serialized Thing (see section* 1.1.3*) to grant access to*
Output	thing:anyURI	*Thing Descriptor of the TMS with security definition (e. g. Bearer authentication)*
verifyUserCredentials(String, String) : String		
Users send credentials for authentication		
Input(s)	username:String	*Username*
	password:String	*Password*

Output	jwt:String	*A JSON Web Token to allow the access to the platform*
discoverThing(String): anyURI		
Request the list of things to TMS		
Input(s)	thingDescriptor: String	*The serialized Thing (see section 1.1.3)*
Output	thing:anyURI	*Thing Descriptor*
consumeTMS (thingID): anyURI		
Request one thing to TMS		
Input(s)	thing ID	*The ID of the requested Thing*
Output	thing:anyURI	*Thing Descriptor*

ThingManagementService Requested Interface				
Provider	**Method**	**Description**	**Input**	**Output**
TrustAuthority	*RegisterInGTA()*	*Register a Things in the GTA*	*String* *Thing Descriptor*	*AnyURI: Thing Descriptor*
	verifyCredentialsIn GTA ()	*User send credentials for authetication*	*String: Username, String: Password*	*String: Json Web Token*
Thing Directory	*discoverThingInTD( )*	*Request the list things in Thing Directory*	*String* *Thing Descriptor*	*AnyURI: Thing Descriptor*
	RegisterInThingDir()	*Register a Things in the Thing Directory*	*String* *Thing Descriptor*	*AnyURI: Thing Descriptor*
	consumeTD()	*Request one thing to Thing Directory*	*Thing/<id>*	*AnyURI: Thing* *Descriptor*
	Consume()	*Ask the new create thing to the thing directory*	*String* *Thing Descriptor*	*AnyURI: Thing Descriptor*
	update()	*upload the endpoint of the Thing Descriptor to be accessed by the gateway*	*String* *Thing Descriptor*	*AnyURI: Thing Descriptor*

MSx	*ConsumeActionInMS()*	*Consume an action on a thing in its Micro Service.*	*Thing/<id>/action*	*Object*

4.2 Things Directory

Description of the component

ThingsDirectory Provided Interface		
discoverThingInTD(String): anyUri		
Request the list things in Thing Directory		
Input(s)	*String*	*Filter*
Output	*[anyUri]*	*List of url of the selected things*
RegisterInThingDir()		
Register a Things in the Thing Directory		
Input(s)	string	*Thing Description*
Output	bool	State of success
consumeTD()		
Request one thing to Thing Directory		
Input(s)	AnyURI	ID of the thing the consume
Output	String	The associated thing description
Insert()		
Ask the new create thing to the thing directory		
Input(s)	Thing Description	The thing Description of the new thing to insert
Output	bool	State of success
Update()		
upload the endpoint of the Thing Descriptor to be accessed by the gateway		
Input	AnyURI	*Thing ID of the thing to modify*
Input(s)	string	*New thing description*
Output	bool	State of success
Delete()		

Consume an action on a thing in its Micro Service		
Input(s)	AnyURI	Thing ID of the thing to modify
Output	bool	State of success

4.3 GK-IntegrationEngine

The GK-IntegrationEngineis the component able to convert raw data, coming from different data sources EHR, sensors, iot devices, wearables etc.), in HL7/FHIR v4.0.1 and RDF representation. Data can be sent to this component invoking the REST APIs that it exposes. For IOT, it accepts as input data in the formats XML, JSON and CVS and provides as output their representation in rdf. The rules for the transformation are written with the language RML using the terminologies provided by the task T3.4. Transformed data is sent to the component RDFSemanticDataLake.

For electronic health record, it converts custom EHR into FHIR v4.0.1 representation according the GK FHIR profiles defined in the task T3.5. Data can be sent to this component invoking the REST APIs that it exposes. GK-IntegrationEngine accepts as input data in the formats XML and JSON and provides as output their representation in FHIR standard (JSON/FHIR). The terminologies to be used for the conversion is provided by the task 4.4. Finally transformed data is sent to the component GK-FHIRService.

IGK-IntegrationEngine Provided Interface

create(pilot: String, sensorId: String, data: File): responseBody: String

Interface accepting data in XML/JSON/CVS format coming from IOT devices (or connector services). If a FHIR processor has been preliminary registered for that device/service, data will be converted and persisted in a FHIR R4 repository. The data will be also converted in RDF and made available in to RDFSemanticDataLake component. If the registered converter produces data complaint to other ontologies (e.g. SAREF) then they will be loaded only in RDFSemanticDataLake repository.

In order to select the appropriate rules to be applied for the transformation, this method accepts as input the name of the pilot, the id of the sensor and a file contacting data.

[POST method]

Input(s)	pilot: String	*The name of pilot. Knowing the name of the pilot this method can apply the right transformation for each pilot. Note that each pilot uses a different data schema*
	sensorId: String	*The id of the sensor. The main goal of this parameter is to select which converter rules should be applied to the data. The pair pilot+sensorId*

		allows to select the specific transformation rules for the data
	data: String	*Actual raw data that must be transformed in RDF and sent to RDFSemanticDataLake. The format of the data can be JSON, XML and CSV. In order to write the rules for the conversion in RDF, it is necessary to know the schema of JSON,XML/CSV.*
Output	String	*data in the new format (XML od JSON)*

create(pilot: String, data: String): responseBody: String

Transforms data in FHIR representation and sends it to GK-FHIRServer component. It returns the output of operation returned by the GK-FHIRServer together with the HTTP codes describing the execution outcome.

This component defines and implements specific conversion rules for each type of data of each use case. In order to select the appropriate rules to be applied for the transformation, this method must know the name of the pilot to which data belong to.

[POST method]

Input(s)	pilot: String	*The name of pilot. Knowing the name of the pilot this method can apply the right transformation for each pilot. Note that each pilot uses a different data schema*
	data: String {json/xml}	*Actual raw data that must be transformed and persisted in the GK-FHIRServer. In order to perform the rules for the transformation in FHIR standard, the structures of the data should be known.* *The format of the data can be JSON or XML. In order to write the rules for the conversion in FHIR standard, it is necessary to know the schema of JSON/XML.*
Output	responseBody: String	*Operation outcome returned by the FHIRServer in JSON/XML format together with the HTTP code that provides feedback about execution outcome.*

IIOTSemanticMappingService Requested Interface				
Provider	**Method**	**Description**	**Input**	**Output**
RDFSemanticDataLake	*create(rdfData: String): HTTPResponse*	*Persist transformed data (RDF) into RDFSemanticDataLake. POST*	*rdfData: String*	*HTTPResponse*
GK-FHIRServer	*create (resource: Bundle): Bundle*	*Send to the GK-FHIRServer raw data (belonging to the pilot) transformed in FHIR standard. It is required that the GK-FHIRServer implement all the operation defined in the FHIR standard. https://hl7.org/FHIR/http.html#operations. POST*	*resource: Bundle*	*Bundle*

4.4 GK-FHIRServer

The GK-FHIR-Server is a component implementing the HL7/FHIR v4.0.1 specification. It provides all RESTful operations described by the standard. Refer to the specification for more details: https://www.hl7.org/fhir/http.html.

This component has been developed using the HAPI FHIR Library (https://hl7.org/FHIR/index.html) that is an open-source implementation of the FHIR specification in Java which defines model classes for every resource type and datatype defined by the standard.

Persisted data are translated in RDF format and sent to the component GK-SemanticDataLake thought its REST APIs.

IFhirServer Provided Interface		
create(resourceType: String, resource: Resource): HTTPResponse		
Create a new resource in a server-assigned location. *POST method*		
Input(s)	resourceType: String	*resource type of the resource to create*

	resource: Resource	*FHIR Resource to create. The resource does not need to have an id element (this is one of the few cases where a resource exists without an id element). If an id is provided, the server SHALL ignore it.*
Output	HTTPResponse	*The server returns a 201 Created HTTP status code, and SHALL also return a Location header which contains the new Logical Id and Version Id of the created resource version*
read(resourceType: String, id: String): resultBody: Resource		
Read the current state of the resource. *GET method*		
Input(s)	resourceType: String	*resource type of the resource to read*
	id: String	*id of Resource*
Output	resource: Resource {json/xml}	*Resource returned by the GK-FHIRServer with the content specified for the resource type in JSON/XML format together with the HTTP code that provides feedback about execution outcome*
vread(resourceType: String, id: String, vid: String): resultBody: Resource		
Read an individual resource instance given a version ID to retrieve a specific version of that instance to vread that instance). *GET method*		
Input(s)	resourceType: String	*resource type of the resource to read*
	id: String	*id of resource*
	vid: String	*version ID to retrieve a specific version of that instance (optional)*
Output	resultBody: Resource {json/xml}	*Resource returned by the GK-FHIRServer with the content specified for the resource type in JSON/XML format together with the HTTP code that provides feedback about execution outcome*
update(resourceType: String, id: String, resource: Resource): resultBody: Resource		
Update an existing resource by its id (or create it if it is new) *PUT method*		
Input(s)	resourceType: String	*resource type of the resource to update*

	id: String	*id of resource*
	resource: Resource	*FHIR Resource to update*
Output	resultBody: Resource {json/xml}	*Resource returned by the GK-FHIRServer with the content specified for the resource type in JSON/XML format together with the HTTP code that provides feedback about execution outcome*
delete(resourceType: String id: String): HTTPResponse		
Delete an individual instance of the resource. DELETE method		
Input(s)	resourceType: String	*resource type of the resource to delete*
	id: String	*id of Resource to delete*
Output	HTTPResponse	*Operation outcome returned by the FHIRServer in JSON/XML format together with the HTTP code that provides feedback about execution outcome*
history(resourceType: String, [id: String]): responseBody: Bundle		
Retrieve the update history for a particular resource type, or against a specific instance of that resource type if an ID is specified. GET method		
Input(s)	resourceType: String	*resource type of the resource to read*
	id: String (optional)	*id of Resource to read*
Output	responseBody: Bundle {json/xml}	*The return content is a Bundle with type set to history containing the specified version history, sorted with oldest versions last, and including deleted resources*
search(resourceType: String, parameters: String[]): responseBody: Bundle		
Search all resources of a particular type using the criteria represented in the parameters. GET method		
Input(s)	resourceType: String	*resource type of the resource to perform the search*
	parameters: String[]	*paremeter of the seach request*
Output	responseBody: Bundle {json/xml}	*The return content is a Bundle the set of the resources fitting the input parameters*

FHIR Server Provided Interface

IFHIRServer Requested Interface				
Provider	**Method**	**Description**	**Input**	**Output**
RDFSemanticDataLake	*create(rdfData: String): HTTPResponse*	*Persist rdf data into RDFSemanticDataLake. POST*	*rdfData: String*	*HTTPResponse*

4.5 RDF Semantic Data Lake

This component is an open source modular Java framework for working with RDF data. This includes parsing, storing, inferencing and querying of/over such data. It offers an easy-to-use API that can be connected to all leading RDF storage solutions. It allows you to connect with SPARQL endpoints and create applications that leverage the power of Linked Data and Semantic Web.

This server should be configured to be compliant to GateKeeper. For now, the only REST operation that it is used is described in the following that allows to store RDF file.

RDFSemanticDataLake provided interface		
create(rdfData: String): HTTPResponse		
REST operation that allows to store RDF file – *POST method*		
Input(s)	rdfData: String	*Rdf data to be persisted*
Output	HTTPResponse	*Http response of the requests*

4.6 Trust Authority

The “TrustAuthority” is the component that will be responsible for validating and certifying the Things of the GateKeeper platform. It will apply validation tests to the “Things” based on a predefined set of specifications that will ensure that a thing respects the rules of the different GATEKEEPER thing profiles (medical device certification, interoperability with standards, GDPR compliance) and levels of trustiness will be calculated as a score. Besides, it will act as a Certification Authority (CA) able to issue digital certificates, which will certify a Thing by giving it the appropriate attributes, and by describing the ownership of a public key by the named subject of the certificate.” Furthermore, it will use a distributed ledger so as to keep an audit trail of all transactions related to things, thus maintaining a detailed history of the whole thing lifecycle. Furthermore, the ledger will track of operations performed on the available data, such as creation, access, deletion and sharing among parties, without access to the actual personal data due to security and regulatory compliance. This component will interact with the "ThingsManagementSystem" to secure all transaction related to Thing lifecycle when an external system (e.g. a User) is authenticated and allowed to perform actions to a "Thing".

TrustAuthority Provided Interface

authenticateUser(domain: string): string

This method will take as an input the domain used by the User in which the User has valid credentials; this domain will be used for the credential validation during the Single sign on mechanism to be used by the User Management module. This method will interact with any GK component that will need to authenticate Users using the User Management module of the GTA component (e.g. the Marketplace)

POST: /authenticateUser

Input(s)	domain:string	*this is a string representing the domain to which the user will be redirected by the User Management module, in order to validate their credentials using the OAuth2.0 mechanism*
Output	authorisation_token:string	*this is a token provided by the User Management that will contain encoded authorisation information about the User based on their certificate issued by the GTA*

registerThing(authorisation_token:string, thing:ThingDescription) file

This method will take as an input an authorisation token string that will contain encoded authorisation information about the User, and a Thing Description (TD) object, and after applying proper Validation of the Thing based on a set of predefined standards, it will produce a validation score. This validation score will be linked with levels of certification and corresponding permissions/roles. A certificate will be issued for the Thing by the Certificate Authority having as an attribute this Validation Score. This method will interact with the TMS

POST: /registerThing

Input(s)	authorisation_token:string	*This is an authorisation token string that will contain encoded authorisation information about the User*
	thing:ThingDescription	*this is the object representing the device, application, service etc. See Thing Description in the Information Model*
Output	Thing Certificate:file	*this is the certificate file (probably in X.509 format) of the Thing as provided by the GTA. It will contain the public key for the Thing as well as the Validation score as attribute of the Certificate*

logAction(string:UserID, string:ThingID, string:ActionType, timestamp:Timestamp)

This method will take as an input a User ID, a Thing ID, and the Type of Action the User wants to perform on the Thing (e.g. register, consume, etc.) and will log this triplet on the

ledger along with the timestamp of the action. This method will be called by the TMS API for logging actions on Things and by the User Management Module for logging actions of Users *POST: /logAction*		
Input(s)	userID	*this is the ID of the User as contained in the Thing Description (TD) of the User*
	thingID	*this is the ID of the Thing as contained in the Thing Description (TD) of the Thing*
	actionType	*this is the a description of the Action the User wants to do on a Thing (e.g. register, consume, etc.)*
	timeStamp	*this is the timestamp when the action was performed by the User in the User Interface, e.g. the timestamp when the User clicked the button to register a new service with the GK Marketplace.)*

Appendix H Third party agreement

This Third Party Agreement, hereinafter the **“Third Party Agreement”** is made on 2021 (“Effective Date”).

BETWEEN:

THE UNIVERSITY OF WARWICK, established in Kirby Corner Road,
University House, COVENTRY CV4 8UW, United Kingdom, VAT number:
GB545270058 (“UoW”)

and

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX **“Third Party”**;

Hereinafter all contracting parties of this Agreement jointly or individually, also referred to as "**Parties**" or “**Party**”;

WHEREAS:

The Coordinator Medtronic Ibérica S.A., together with other Beneficiaries has been awarded a Grant Agreement by the European Commission (“Funding Authority”) no. 857223 entitled ‘Smart Living Homes - Whole Interventions Demonstrator For People At Health And Social Risks’ in short: “GATEKEEPER”, hereinafter referred to as the “Grant Agreement”. From this Grant Agreement including its Annexes certain rights and obligations result between the Funding Authority, the Coordinator and the other GATEKEEPER Beneficiaries. The Grant Agreement states that third parties will be selected and financially supported for certain work to the project.

Whereas, UoW is one of the Beneficiaries of the GATEKEEPER project who, according to the provisions of the Grant Agreement, has the task to provide the financial support of the GATEKEEPER Beneficiaries to the Third Party for their services to the project Under the Grant Agreement, the GATEKEEPER Beneficiaries are required to ensure that the GATEKEEPER Project is implemented in compliance with the provisions of the Grant Agreement; and the Parties shall comply with this in implementation of their tasks. The GATEKEEPER Beneficiaries including the Coordinator furthermore have entered into a Consortium Agreement dated XXXXXXX by which they have obligations towards each other. The Third Party shall not do anything or omit to do anything which renders UoW or the Coordinator or the other GATEKEEPER Beneficiaries in breach of the Grant Agreement or the Consortium Agreement. For the avoidance of doubt, “Beneficiaries” means all partners who have signed the Grant Agreement, i.e. including the Coordinator Medtronic Ibérica S.A. and UoW.

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1 Definitions

Words beginning with a capital letter shall have the meaning defined either herein or in the Rules of Participation for Horizon 2020 or in the Grant Agreement or Consortium Agreement, including their respective Appendixes.

2 Subject

2.1 The Third Party will perform the work using reasonable care and skill and as defined in this Third Party Agreement, the Grant Agreement, and as offered by the Third Party and finally agreed with UoW. The offer of the Third Party is attached to this Third Party Agreement as Appendix 1.

2.2 The Third Party shall be responsible for ensuring that the work is carried out and complies with accepted technical, scientific and professional standards, is undertaken by appropriate personnel and carried out in accordance with the Grant Agreement.

2.3 Each Third Party assumes all responsibility towards UoW for all tasks contracted to it by this Third Party Agreement and shall indemnify UoW in case of breach of its obligations.

2.4 Additionally, each Third Party recognizes that UoW and the other GATEKEEPER Beneficiaries are bound by certain obligations arising out of the Grant Agreement and the GATEKEEPER Consortium Agreement. Notwithstanding any other term of this Third Party Agreement, the Third Party will at all times use all reasonable endeavours to facilitate and allow UoW's and the other GATEKEEPER Beneficiary's compliance with the terms of the Grant Agreement and Consortium Agreemetn. Herewith, each Third Party agrees to comply with all obligations arising out of the Grant Agreement and the GATEKEEPER Consortium Agreement.

2.5 Each Third Party accepts the Terms and Conditions of the Grant Agreement and of the GATEKEEPER Consortium Agreement as if they were a party to it and insofar as they relate to the tasks which are contracted to it hereby. The principal Terms and Conditions of the Grant Agreement are attached as Appendix 2 to this Third Party Agreement.

3 Duration

3.1 The GATEKEEPER Project has started on 1st October 2019 with a duration of 42 months. This Third Party Agreement will be effective from the Effective Date first mentioned above and will be valid as long as the Grant Agreement. Should the period of validity of the Grant Agreement be amended, this Third Party Agreement shall be deemed automatically changed accordingly.

The Third Party shall commence to perform its activities according to the plan in Appendix 1 on <date> and shall have completed it on <date>. By that date all results and reports shall have been delivered to UoW.

3.2 During the term of this Third Party Agreement, the Third Party shall provide UoW with regular updates which summarise the progress of the Third Party Project. The Third Party shall notify UoW in writing without undue delay if it becomes aware that it might be a delay in performing its obligations, and the plan in Appendix 1, under this Agreement.

3.3 UoW can terminate this Agreement with immediate effect through written notice to the Third Party:

- if the Third Party is in breach of any of its material obligations under this Third Party Agreement, which breach is not remediable, or, if remediable, has not been remedied within thirty (30) days after written notice of UoW about the breach,
- if, to the extent permitted by law, the Third Party is declared bankrupt, is being wound up, is having its affairs administered by the courts, has entered into an arrangement with its creditors, has suspended business activities, or is the subject of any other similar proceeding concerning those matters, or
- if the Third Party is subject to an event of Force Majeure (in accordance with how that term is defined under Article 51 of the Grant Agreement), which prevents the Third Party from correct performance of its obligations hereunder and such circumstances have lasted, or can reasonably be expected to last more than six (6) weeks.

4 Financial Provisions regarding Financial Support to the Third Party

4.1 The tasks allocated to the Third Party are paid as a lump sum as indicated hereinafter:

XXXXXXXXXXXX EUR

The payment schedule, which contains the transfer of pre-financing and interim payments to Parties, will be handled according to the following:

- Funding of costs included in the Consortium Plan will be paid to Parties after receipt from the Coordinator or Funding Authority without undue delay and in conformity with the provisions of the Grant Agreement. Costs accepted by the Funding Authority will be paid to the Party concerned.
- UoW is entitled to withhold any payments due to the Third Party if it is identified by a responsible Consortium Body to be in breach of its obligations under this Third Party Agreement or the Grant Agreement
- UoW is entitled to recover any payments already paid to a Defaulting Party, except for costs accepted by the Funding Authority. UoW is equally entitled to withhold payments to a Third Party when this is suggested by or agreed with the Funding Authority.

Payments of the lump sum will be made in three instalments: 20% as pre-financing, 50% at mid-term and the remaining 30% at the end of the project, the midterm and final payments upon approval of the respective milestone(s) and deliverable(s), as well as receipt of the Third Party's payment request.

Each payment request must include detailed information on the Third Party's spending e.g. costs for travel/accommodation, consumables and equipment.

At the time a payment request is submitted, written documentation must be provided to UoW for the completion and proper implementation of the corresponding deliverable and/or progress.

The Third Party shall account for its costs in accordance with Article 15 of the Grant Agreement in its own responsibility.

4.2The budget in Annex 2 of the Grant Agreement, including all amendments which may occur throughout the project duration, shall apply to this Third Party Agreement as far as the tasks allocated to the Third Party are affected.

4.3Taking into account the above-mentioned clauses, UoW will forward the payments received by the Funding Authority for the costs stated by the Third Party on to a Third Party' s bank account stated in Appendix 3 after approval of the costs in accordance with this Third Party Agreement and the Grant Agreement.

5 Organisation and Performance of the Work

5.1 Technical and Financial Responsibility

The Third Party shall provide all personnel, facilities, equipment and materials necessary for the proper performance of this Third Party Agreement and shall assume the technical and financial responsibility for the work specified in Appendix 1. Each Third Party undertakes to indemnify UoW and/or other GATEKEEPER Beneficiaries against any failure on its part to discharge its aforementioned responsibilities.

5.2 Technical and Financial Control, Verification, Audits

Each Third Party undertakes to supply UoW and/or other GATEKEEPER Beneficiaries without delay with any information which the latter may request concerning the implementation of this Third Party Agreement. In particular, upon request the Third Party shall make available to UoW, the other GATEKEEPER Beneficiaries and to their auditors the technical and financial documents verifying the costs and that the work is being or has been carried out. Each Third Party acknowledges and accepts the rights of the Funding Authority relating to controls and audits laid down in Articles 22 and 23 of the Grant Agreement.

Each Third Party undertakes to give the representatives of UoW reasonable access to the premises where the work is being carried out and to all documents concerning the work programme and/or necessary to verify the compliance with the obligations arising from this Third Party Agreement and of the Grant Agreement including its Annexes. Additionally, the Third Party acknowledges and accepts the rights of the European Commission and/or its agencies, the Court of Auditors or any third party authorised by the European Commission and/or its agencies relating to the technical and financial or other verification of this Third Party Agreement laid down in Articles 22 and 23 of the Grant Agreement.

5.3 Each Third Party fully accepts and will abide by the provisions of the Grant Agreement, specifically the provisions of Articles 22, 35, 36, 38, 39 and 46 of the Grant Agreement, as attached at Appendix 2.

6 Results

6.1 Ownership of Results

Results are owned by the Party or the GATEKEEPER Beneficiary that generates them.

6.2 Joint ownership

Joint ownership is governed by Grant Agreement Article 26.2 with the following additions:

Unless otherwise agreed:
- each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s), and
- each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and
to grant non-exclusive licenses to third parties (without any right to sub-license), if the other
joint owners are given:
(a) at least 45 calendar days advance notice; and
(b) Fair and Reasonable compensation.

The joint owners shall agree on all protection measures and the division of related cost in advance.

Notwithstanding the foregoing, STMicroelectronics (Alps) SAS will not apply for joint patents
with other Parties under this Consortium Agreement. In case STMicroelectronics (Alps) SAS
has a joint patentable result with another Party(ies), then the Parties concerned will negotiate
the ownership of the property of such joint patent to one of them, with a right for the other
Party(ies) to continue the exploitation of such patent under the conditions to be negotiated
between the Parties concerned.

7 Access Rights

The Third Party shall grant a non-exclusive, royalty-free, transferable and unlimited access right of use with the right for sub-licensing to UoW and the other GATEKEEPER Beneficiaries for implementation of the GATEKEEPER Project with regard to all results achieved by the Third Party in the course of the work according to this Third Party Agreement ("Third Party Results") and with regard to the Background of the Third Party related to these Third Party Results. If UoW and/or the other GATEKEEPER Beneficiaries need to use Third Party Results and/or the related Background of a Third Party for use or commercial exploitation of their own Results of the GATEKEEPER Project, each Third Party shall grant a non-exclusive, transferable right of use with regard to Third Party Results and related Background based on Fair and Reasonable Conditions.

The Third Party shall use all reasonable endeavours to ensure the accuracy of all information and data provided by it to UoW and/or other GATEKEEPER Beneficiaries under this Third Party Agreement, whether they are Third Party Results or not and whether they are protected by intellectual property rights or not, and warrants its right to disclose such information. In the event of any error or omission in the Third Party Results being brought to the attention of the Third Party by UoW or the other GATEKEEPER Beneficiaries, the Third Party undertakes to correct such error or rectify such omission promptly, during which time UoW shall be entitled to withhold payment of any sums due to the Third Party.

The Third Party warrants that the Results and any information provided by it under this Third Party Agreement shall to the best of it's reasonable knowledge and belief not infringe the intellectual property rights of any third party, and shall indemnify UoW and the other GATEKEEPER Beneficiaries fully and effectively from any and all liabilities, costs expenses, howsoever arising from breach of this warranty.

8 Dissemination

Each Party agrees that any dissemination activity (including publications, presentations or contributions to any standards organisation) by the Third Party is subject to the prior written approval of UoW and the other GATEKEEPER Beneficiaries and in accordance with Clause 8.4 of the Consortium Agreement.

9 Confidentiality

9.1 All information in whatever form or mode of communication, which is disclosed by a Party (the "Disclosing Party") to any other Party (the "Recipient") in connection with this Third Party Agreement and the tasks of the Third Party and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 15 calendar days from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information".

9.2 The Recipients hereby undertake for a period of 5 years after the termination of this Third Party Agreement:

- not to use Confidential Information otherwise than for the purpose for which it was disclosed;
- except to the extent expressly set forth herein for implementation, not to disassemble, radiograph, reverse engineer or otherwise analyze (in relation to its physical, chemical or other characteristics and/or components) in whole or in party any Confidential Information provided by the Disclosing Party without prior written consent of the Disclosing Party
- not to disclose Confidential Information without the prior written consent by the Disclosing Party;
- to ensure that internal distribution of Confidential Information by a Recipient to its employees, Affiliated Entities and Subcontractors shall take place on a strict need-to-know basis; and whereby the Recipient must ensure that an arrangement is in place prior

to such disclosure that subjects the employees, Affiliated Entities and/or Subcontractors to provisions at least as strict as provided in this Section 10; and
- to return to the Disclosing Party, or destroy, on request all Confidential Information that has been disclosed to the Recipients including all copies thereof and to delete all information stored in a machine readable form to the extent practically possible. The Recipients may keep a copy to the extent it is required to keep, archive or store such Confidential Information because of compliance with applicable laws and regulations or for the proof of on-going obligations provided that the Recipient comply with the confidentiality obligations herein contained with respect to such copy for as long as the copy is retained.

9.3 The Recipients shall be responsible for the fulfilment of the above obligations on the part of their employees or third parties involved in implementing the tasks and shall ensure that they remain so obliged, as far as legally possible, during and after the end of this Third Party Agreement and/or after the termination of the contractual relationship with the employee or third party.

9.4 The above shall not apply for disclosure or use of Confidential Information, if and in so far as the Recipient can show that:
- the Confidential Information has become or becomes publicly available by means other than a breach of the Recipient's confidentiality obligations;
- the Disclosing Party subsequently informs the Recipient that the Confidential Information is no longer confidential;
- the Confidential Information is communicated to the Recipient without any obligation of confidentiality by a third party who is to the best knowledge of the Recipient in lawful possession thereof and under no obligation of confidentiality to the Disclosing Party;
- the disclosure or communication of the Confidential Information is foreseen by provisions of the Grant Agreement;
- the Confidential Information, at any time, was developed by the Recipient completely independently of any such disclosure by the Disclosing Party;
- the Confidential Information was already known to the Recipient prior to disclosure, or
- the Recipient is required to disclose the Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order. If a Party becomes aware that it will be required, or is likely to be required, to disclose Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order, it shall, to the extent it is lawfully able to do so, prior to any such disclosure notify the Disclosing Party, and comply with the Disclosing Party's reasonable instructions to protect the confidentiality of the information.

9.5 The Recipient shall apply the same degree of care with regard to the disclosed Confidential Information as with its own confidential and/or proprietary information, but in no case less than reasonable care

9.6 Each Party shall promptly advise the other Party in writing of any unauthorised disclosure, misappropriation or misuse of Confidential Information after it becomes aware of such unauthorised disclosure, misappropriation or misuse.

9.7 The same obligations of confidentiality apply to the Third Party who is receiving Confidential Information by the other GATEKEEPER Beneficiaries.

10 Reports and Deliverables

10.1 The Third Party agrees to submit progress reports to UoW and the responsible work package leader of the GATEKEEPER Beneficiaries to enable UoW and/or the other GATEKEEPER Beneficiaries to include all contents directly into the project reporting, and to identify work performed and resources deployed by the Third Party. UoW also reserves the right to forward the report of the Third Party directly to the Funding Authority.

10.2 The contents and format of the various reports required will be agreed between UoW and/or other GATEKEEPER Beneficiaries and the Third Party based on the conditions of the Grant Agreement.

11 Liability

11.1 UoW´s liability

The contractual liability of UoW under this Third Party Agreement shall in any case be limited to the amount of the financial support provided or to be provided to the Third Party hereunder. UoW shall not in any case be liable for any indirect or consequential damages such as:

- loss of profits, interest, savings, shelf-space, production and business opportunities;
- lost contracts, goodwill, and anticipated savings;
- loss of or damage to reputation or to data;
- costs of recall of products; or
- any other type of indirect, incidental, punitive, special or consequential loss or damage.

This limitation of liability shall not apply in cases of wilful act or gross negligence.

11.2 Liability between Third Party, UoW and the other GATEKEEPER Beneficiaries

The Third Party shall fully and exclusively bear the risks in connection with the work provided by it and for which financial support is granted and forwarded by UoW. The Third Party shall indemnify UoW and the other GATEKEEPER Beneficiaries for all damages, penalties, costs and expenses which UoW or a GATEKEEPER Beneficiary as a result thereof would incur or have to pay to the European Commission or to any third parties with respect to the Third Party's work financially supported and/or for any damage in general which UoW or the GATEKEEPER Beneficiaries incur as a result thereof.

The Third Party indemnifies UoW without limit should the Funding Authority claim any reimbursement of any of the funding or terminate the Grant Agreement, or should any indemnity be payable by UoW to the Funding Authority, as a result of any failure on the part of The Third Party to properly implement the Third Party work or to comply with the terms and conditions of the Grant Agreeemnet.

Moreover, the Third Party shall indemnify UoW and the GATEKEEPER Beneficiaries, their respective officers, directors, employees and agents from and against all repayments, loss, liability, costs, charges, claims or damages that result from or arising out of any such recovery action by the Funding Authority.

Should any GATEKEEPER Beneficiary make any claim towards UoW under UoW's overall responsibility for the Third Party' tasks in accordance with Article 15 in the Grant Agreement, the Third Party shall indemnify UoW from any costs.

12 Miscellaneous

12.1 Attachments, inconsistencies and severability

In case the terms of this Agreement are in conflict with the terms of the Grant Agreement, the terms of the latter shall prevail.

Should any provision of this Agreement become invalid, illegal or unenforceable, it shall not affect the validity of the remaining provisions of this Agreement. In such a case, the Parties concerned shall be entitled to request that a valid and practicable provision be negotiated which fulfils the purpose of the original provision.

This Agreement shall immediately terminate if the Grant Agreement is terminated. Clauses 6, 7, 8, 9, 11 remain valid also after expiration or termination of this Third Party Agreement.

12.2 No representation, partnership or agency

No Party shall be entitled to act or to make legally binding declarations on behalf of any other Party. Furthermore, a Third Party shall not be entitled to act or to make legally binding declarations on behalf of any of the GATEKEEPER Beneficiaries. Nothing in this Agreement shall be deemed to constitute a joint venture, agency, partnership, interest grouping or any other kind of formal business grouping or entity between the Parties.

12.3 Mandatory national law

Nothing in this Agreement shall be deemed to require a Party to breach any mandatory statutory law under which the Party is operating.

12.4 Language

This Agreement is drawn up in English, which language shall govern all documents, notices, meetings, arbitral proceedings and processes relative thereto.

12.5 Applicable law and settlement of disputes

This Agreement shall be construed in accordance with and governed by the laws of Belgium excluding its conflict of law provisions.

The parties shall endeavour to settle their disputes amicably. If a dispute concerning the interpretation, application or validity of this Agreement cannot be settled amicably, the General Court in Brussels, Belgium will have jurisdiction. Nothing in this Consortium Agreement shall limit the Parties' right to seek injunctive relief in any applicable competent court.

12.6 Export Control

The Third Party agrees that access to Results and licensed products under this Third Party Agreement is granted with the specific understanding and requirement that responsibility for ensuring compliance with all applicable UK and foreign export laws and regulations are being undertaken by the parties. This responsibility includes an obligation to ensure that any individual receiving access hereunder who is not a UK citizen or permanent UK resident is permitted access under applicable UK and foreign export laws and regulations. The Third Party further understands and acknowledges their obligations to make a prompt report to each other and appropriate authorities regarding any access to or use of Results and licensed products hereunder that maybe in violation of applicable UK and foreign export laws and regulations. In addition, the Third Party hereby agrees that no licensed products, technical data, know-how or other information or assistance furnished pursuant to this Third Party Agreement, or any product or revision thereof, shall be re-exported or otherwise used by another Third Party or its authorized transferees outside of the Third Party's principal domiciliary country. These obligations shall survive any satisfaction, expiration, termination, or discharge of this Third Party Agreement or any other obligations.

12.7 Data Protection

The Third Party shall comply at all times with the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 (whilst the same is still in force in England and Wales), and any relevant replacement/subsequent European and/or UK privacy legislation, for the purposes of performing its obligations and exercising its rights under these terms and conditions ("Data Protection Laws") and shall not perform its obligations under this Collaboration Agreement in such a way as to cause any other Party to breach any of its obligations under the Data Protection Legislation.

In the event that the Third Party receives personal data in connection with this Third Party Agreement and its subject matter, the Third Party hereby warrants that any sharing, use and other processing of Personal Data shall be done only in accordance with the Data Protection Laws.

Signatures

AS WITNESS:

The Parties have caused this Agreement to be duly signed by the undersigned authorised representatives in separate signature pages the day and year first above written.

UNIVERSITY OF WARWICK as Beneficiary in the GATEKEEPER Project

Signature(s)

Name

Date

Third Party

XXXXXXXXX

Signature(s)

Name

Title

Date

Appendix 1 - Third Party Proposal

[ADD A COPY OF THE PROPOSAL HERE]

Appendix 2 – Excerpts from the Grant Agreement – principal Terms and Conditions:

ARTICLE 22 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS

22.1 Checks, reviews and audits by the Commission

22.1.1 Right to carry out checks

The Commission will — during the implementation of the action or afterwards — check the proper

implementation of the action and compliance with the obligations under the Agreement, including

assessing deliverables and reports.

For this purpose the Commission may be assisted by external persons or bodies.

The Commission may also request additional information in accordance with Article 17. The Commission may request beneficiaries to provide such information to it directly. Information provided must be accurate, precise and complete and in the format requested, including electronic format.

22.1.2 Right to carry out reviews

The Commission may — during the implementation of the action or afterwards — carry out reviews on the proper implementation of the action (including assessment of deliverables and reports), compliance with the obligations under the Agreement and continued scientific or technological relevance of the action. Reviews may be started up to two years after the payment of the balance. They will be formally notified to the coordinator or beneficiary concerned and will be considered to have started on the date of the formal notification. If the review is carried out on a third party (see Articles 10 to 16), the beneficiary concerned must inform the third party. The Commission may carry out reviews directly (using its own staff) or indirectly (using external persons or bodies appointed to do so). It will inform the coordinator or beneficiary concerned of the identity of the external persons or bodies. They have the right to object to the appointment on grounds of commercial confidentiality. The coordinator or beneficiary concerned must provide — within the deadline requested — any information and data in addition to deliverables and reports already submitted (including information on the use of resources). The Commission may request beneficiaries to provide such information to it directly. The coordinator or beneficiary concerned may be requested to participate in meetings, including with external experts. For on-the-spot reviews, the beneficiaries must allow access to their sites and premises, including to external persons or bodies, and must ensure that information requested is readily available. Information provided must be accurate, precise and complete and in the format requested, including electronic format. On the basis of the review findings, a 'review report' will be drawn up. The Commission will formally notify the review report to the coordinator or beneficiary concerned,

which has 30 days to formally notify observations ('contradictory review procedure'). Reviews (including review reports) are in the language of the Agreement.

22.1.3 Right to carry out audits

The Commission may — during the implementation of the action or afterwards — carry out audits on the proper implementation of the action and compliance with the obligations under the Agreement.

Audits may be started up to two years after the payment of the balance. They will be formally notified to the coordinator or beneficiary concerned and will be considered to have started on the date of the formal notification.

If the audit is carried out on a third party (see Articles 10 to 16), the beneficiary concerned must inform the third party.

The Commission may carry out audits directly (using its own staff) or indirectly (using external persons or bodies appointed to do so). It will inform the coordinator or beneficiary concerned of the identity of the external persons or bodies. They have the right to object to the appointment on grounds of commercial confidentiality. The coordinator or beneficiary concerned must provide — within the deadline requested — any information (including complete accounts, individual salary statements or other personal data) to verify compliance with the Agreement. The Commission may request beneficiaries to provide such

information to it directly.

For on-the-spot audits, the beneficiaries must allow access to their sites and premises, including to external persons or bodies, and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the audit findings, a ‘draft audit report’ will be drawn up.

The Commission will formally notify the draft audit report to the coordinator or beneficiary concerned, which has 30 days to formally notify observations (‘contradictory audit procedure’). This period may be extended by the Commission in justified cases.

The ‘final audit report’ will take into account observations by the coordinator or beneficiary concerned. The report will be formally notified to it.

Audits (including audit reports) are in the language of the Agreement. The Commission may also access the beneficiaries’ statutory records for the periodical assessment of unit costs or flat-rate amounts.

22.2 Investigations by the European Anti-Fraud Office (OLAF)

Under Regulations No 883/201316 and No 2185/9617 (and in accordance with their provisions and procedures), the European Anti-Fraud Office (OLAF) may — at any moment during implementation of the action or afterwards — carry out investigations, including on-the-spot checks and inspections, to establish whether there has been fraud, corruption or any other illegal activity affecting the financial

interests of the EU.

22.3 Checks and audits by the European Court of Auditors (ECA)

Under Article 287 of the Treaty on the Functioning of the European Union (TFEU) and Article 161 of the Financial Regulation No 966/201218, the European Court of Auditors (ECA) may — at any moment during implementation of the action or afterwards — carry out audits.

The ECA has the right of access for the purpose of checks and audits.

22.4 Checks, reviews, audits and investigations for international organisations

Not applicable

22.5 Consequences of findings in checks, reviews, audits and investigations — Extension of findings

22.5.1 Findings in this grant

Findings in checks, reviews, audits or investigations carried out in the context of this grant may lead to the rejection of ineligible costs (see Article 42), reduction of the grant (see Article 43), recovery of undue amounts (see Article 44) or to any of the other measures described in Chapter 6.

Rejection of costs or reduction of the grant after the payment of the balance will lead to a revised final grant amount (see Article 5.4).

Findings in checks, reviews, audits or investigations may lead to a request for amendment for the modification of Annex 1 (see Article 55).

Checks, reviews, audits or investigations that find systemic or recurrent errors, irregularities, fraud or breach of obligations may also lead to consequences in other EU or Euratom grants awarded under similar conditions ('extension of findings from this grant to other grants').

Moreover, findings arising from an OLAF investigation may lead to criminal prosecution under national law.

22.5.2 Findings in other grants

The Commission may extend findings from other grants to this grant ('extension of findings from other grants to this grant'), if:

(a) the beneficiary concerned is found, in other EU or Euratom grants awarded under similar conditions, to have committed systemic or recurrent errors, irregularities, fraud or breach of obligations that have a material impact on this grant and

(b) those findings are formally notified to the beneficiary concerned — together with the list of grants affected by the findings — no later than two years after the payment of the balance of this grant.

The extension of findings may lead to the rejection of costs (see Article 42), reduction of the grant (see Article 43), recovery of undue amounts (see Article 44), suspension of payments (see Article 48), suspension of the action implementation (see Article 49) or termination (see Article 50).

22.5.3 Procedure

The Commission will formally notify the beneficiary concerned the systemic or recurrent errors and its intention to extend these audit findings, together with the list of grants affected.

22.5.3.1 If the findings concern eligibility of costs: the formal notification will include:

(a) an invitation to submit observations on the list of grants affected by the findings;

(b) the request to submit revised financial statements for all grants affected;

(c) the correction rate for extrapolation established by the Commission on the basis of the systemic or recurrent errors, to calculate the amounts to be rejected if the beneficiary concerned:

(i) considers that the submission of revised financial statements is not possible or practicable

or

(ii) does not submit revised financial statements.

The beneficiary concerned has 90 days from receiving notification to submit observations, revised financial statements or to propose a duly substantiated alternative correction method. This periodmay be extended by the Commission in justified cases.

The Commission may then start a rejection procedure in accordance with Article 42, on the basis of:

- the revised financial statements, if approved;

- the proposed alternative correction method, if accepted

or

- the initially notified correction rate for extrapolation, if it does not receive any observations or revised financial statements, does not accept the observations or the proposed alternative correction method or does not approve the revised financial statements.

22.5.3.2 If the findings concern substantial errors, irregularities or fraud or serious breach of obligations: the formal notification will include:

(a) an invitation to submit observations on the list of grants affected by the findings and

(b) the flat-rate the Commission intends to apply according to the principle of proportionality.

The beneficiary concerned has 90 days from receiving notification to submit observations or to propose a duly substantiated alternative flat-rate.

The Commission may then start a reduction procedure in accordance with Article 43, on the basis of:

- the proposed alternative flat-rate, if accepted

or

the initially notified flat-rate, if it does not receive any observations or does not accept the observations or the proposed alternative flat-rate.

22.6 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, any insufficiently substantiated costs

will be ineligible (see Article 6) and will be rejected (see Article 42).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 23 — EVALUATION OF THE IMPACT OF THE ACTION

23.1 Right to evaluate the impact of the action

The Commission may carry out interim and final evaluations of the impact of the action measured against the objective of the EU programme.

Evaluations may be started during implementation of the action and up to five years after the payment of the balance. The evaluation is considered to start on the date of the formal notification to the coordinator or beneficiaries.

The Commission may make these evaluations directly (using its own staff) or indirectly (using external bodies or persons it has authorised to do so).

The coordinator or beneficiaries must provide any information relevant to evaluate the impact of the action, including information in electronic format.

23.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the *Agency* may apply the measures described in Chapter 6.

ARTICLE 35 — CONFLICT OF INTERESTS

35.1 Obligation to avoid a conflict of interests

The beneficiaries must take all measures to prevent any situation where the impartial and objective implementation of the action is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest ('**conflict of interests**').

They must formally notify to the Commission without delay any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation. The Commission may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

35.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43) and the Agreement or participation of the beneficiary may be terminated (see Article 50). Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 36 — CONFIDENTIALITY

36.1 General obligation to maintain confidentiality

During implementation of the action and for four years after the period set out in Article 3, the parties must keep confidential any data, documents or other material (in any form) that is identified as confidential at the time it is disclosed ('**confidential information**').

If a beneficiary requests, the Commission may agree to keep such information confidential for an additional period beyond the initial four years.

If information has been identified as confidential only orally, it will be considered to be confidential only if this is confirmed in writing within 15 days of the oral disclosure.

Unless otherwise agreed between the parties, they may use confidential information only to implement the Agreement.

The beneficiaries may disclose confidential information to their personnel or third parties involved in the action only if they:

(a) need to know to implement the Agreement and

(b) are bound by an obligation of confidentiality.

This does not change the security obligations in Article 37, which still apply.

The Commission may disclose confidential information to its staff, other EU institutions and bodies. It may disclose confidential information to third parties, if:

(a) this is necessary to implement the Agreement or safeguard the EU's financial interests and

(b) the recipients of the information are bound by an obligation of confidentiality.

Under the conditions set out in Article 4 of the Rules for Participation Regulation No 1290/2013, the Commission must moreover make available information on the results to other EU institutions, bodies, offices or agencies as well as Member States or associated countries.

The confidentiality obligations no longer apply if:

(a) the disclosing party agrees to release the other party;

(b) the information was already known by the recipient or is given to him without obligation of confidentiality by a third party that was not bound by any obligation of confidentiality;

(c) the recipient proves that the information was developed without the use of confidential information;

(d) the information becomes generally and publicly available, without breaching any confidentiality obligation, or

(e) the disclosure of the information is required by EU or national law.

36.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 38 — PROMOTING THE ACTION — VISIBILITY OF EU FUNDING

38.1 Communication activities by beneficiaries

38.1.1 Obligation to promote the action and its results

The beneficiaries must promote the action and its results, by providing targeted information to multiple audiences (including the media and the public) in a strategic and effective manner.

This does not change the dissemination obligations in Article 29, the confidentiality obligations in Article 36 or the security obligations in Article 37, all of which still apply.

Before engaging in a communication activity expected to have a major media impact, the beneficiaries must inform the Commission (see Article 52).

38.1.2 Information on EU funding — Obligation and right to use the EU emblem

Unless the Commission requests or agrees otherwise or unless it is impossible, any communication activity related to the action (including in electronic form, via social media, etc.) and any infrastructure, equipment and major results funded by the grant must:

(a) display the EU emblem and

(b) include the following text:

> For communication activities: "This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No No 857223".

> For infrastructure, equipment and major results: "This [infrastructure][equipment][insert type of result] is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No No 857223".

When displayed together with another logo, the EU emblem must have appropriate prominence.

For the purposes of their obligations under this Article, the beneficiaries may use the EU emblem without first obtaining approval from the Commission.

This does not, however, give them the right to exclusive use.

Moreover, they may not appropriate the EU emblem or any similar trademark or logo, either by registration or by any other means.

38.1.3 Disclaimer excluding the Commission responsibility

Any communication activity related to the action must indicate that it reflects only the author's view and that the Commission is not responsible for any use that may be made of the information it contains.

38.2 Communication activities by the Commission

38.2.1 Right to use beneficiaries' materials, documents or information

The Commission may use, for its communication and publicising activities, information relating to the action, documents notably summaries for publication and public deliverables as well as any other material, such as pictures or audio-visual material that it receives from any beneficiary (including in electronic form).

This does not change the confidentiality obligations in Article 36 and the security obligations in Article 37, all of which still apply.

If the Commission's use of these materials, documents or information would risk compromising legitimate interests, the beneficiary concerned may request the Commission not to use it (see Article 52).

The right to use a beneficiary's materials, documents and information includes:

(a) **use for its own purposes** (in particular, making them available to persons working for the Commission or any other EU institution, body, office or agency or body or institutions in EU Member States; and copying or reproducing them in whole or in part, in unlimited numbers);

(b) **distribution to the public** (in particular, publication as hard copies and in electronic or digital format, publication on the internet, as a downloadable or non-downloadable file, broadcasting by any channel, public display or presentation, communicating through press information services, or inclusion in widely accessible databases or indexes);

(c) **editing or redrafting** for communication and publicising activities (including shortening, summarising, inserting other elements (such as meta-data, legends, other graphic, visual, audio or text elements), extracting parts (e.g. audio or video files), dividing into parts, use in a compilation);

(d) **translation**;

(e) giving **access in response to individual requests** under Regulation No 1049/2001, without the right to reproduce or exploit;

(f) **storage** in paper, electronic or other form;

(g) **archiving**, in line with applicable document-management rules, and

(h) the right to authorise **third parties** to act on its behalf or sub-license the modes of use set out in Points (b), (c), (d) and (f) to third parties if needed for the communication and publicising activities of the Commission.

If the right of use is subject to rights of a third party (including personnel of the beneficiary), the beneficiary must ensure that it complies with its obligations under this Agreement (in particular, by obtaining the necessary approval from the third parties concerned).

Where applicable (and if provided by the beneficiaries), the Commission will insert the following information:

"© – [year] – [name of the copyright owner]. All rights reserved. Licensed to the European Union (EU) under conditions."

38.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 46 — LIABILITY FOR DAMAGES

46.1 Liability of the Commission

The Commission cannot be held liable for any damage caused to the beneficiaries or to third parties as a consequence of implementing the Agreement, including for gross negligence.

The Commission cannot be held liable for any damage caused by any of the beneficiaries or third parties involved in the action, as a consequence of implementing the Agreement.

46.2 Liability of the beneficiaries

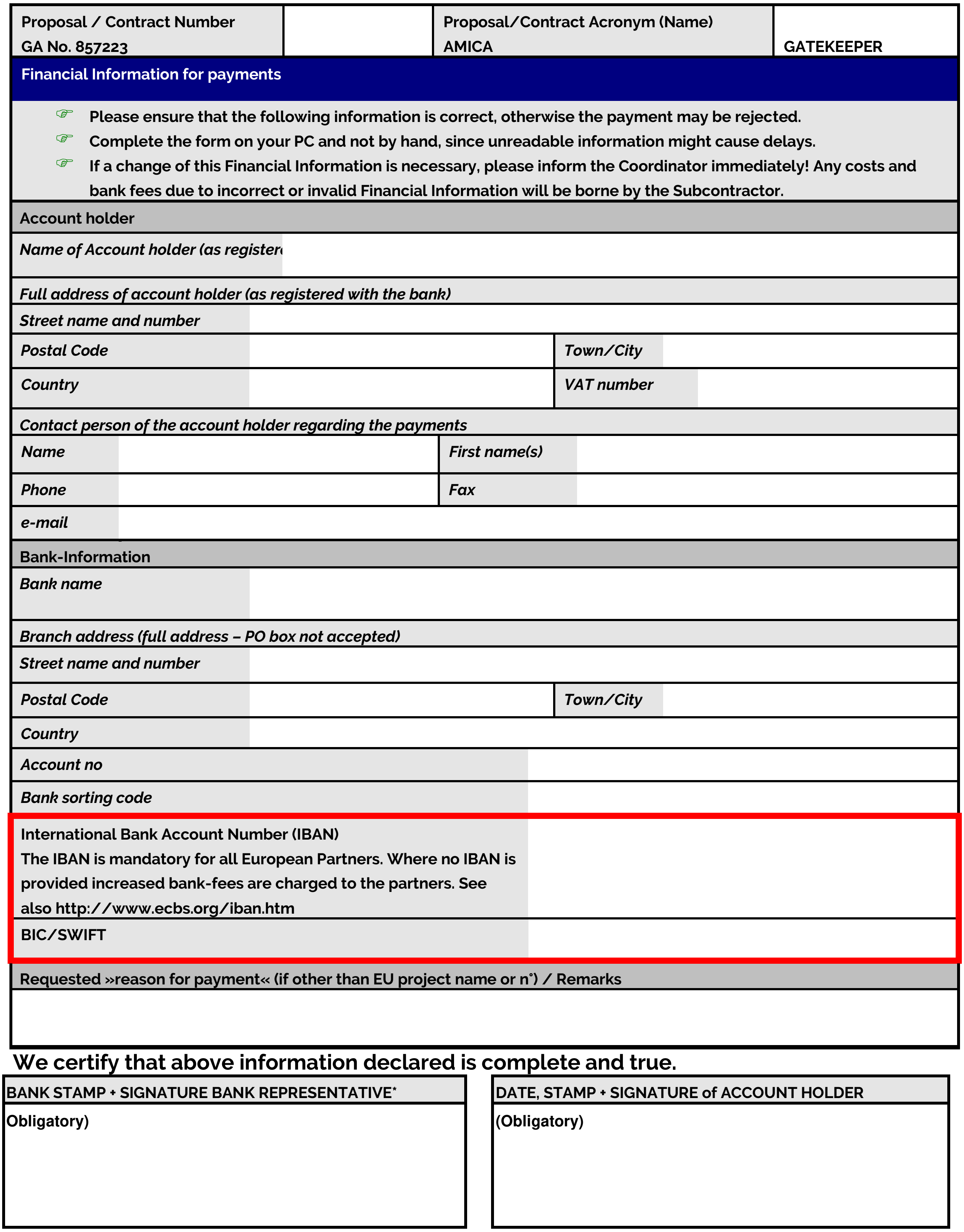
Except in case of force majeure (see Article 51), the beneficiaries must compensate the Commission for any damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement.

Appendix 3

Banking Information Form

Information of the Third Party concerning the Third Party Agreement relating to GATEKEEPER, Grant Agreement No.: 857223

(see next page)



Proposal / Contract Number GA No. 857223		Proposal/Contract Acronym (Name) AMICA	GATEKEEPER

Financial Information for payments

- ☞ Please ensure that the following information is correct, otherwise the payment may be rejected.
- ☞ Complete the form on your PC and not by hand, since unreadable information might cause delays.
- ☞ If a change of this Financial Information is necessary, please inform the Coordinator immediately! Any costs and bank fees due to incorrect or invalid Financial Information will be borne by the Subcontractor.

Account holder

Name of Account holder (as register			
Full address of account holder (as registered with the bank)			
Street name and number			
Postal Code		*Town/City*	
Country		*VAT number*	
Contact person of the account holder regarding the payments			
Name		*First name(s)*	
Phone		*Fax*	
e-mail			

Bank-Information

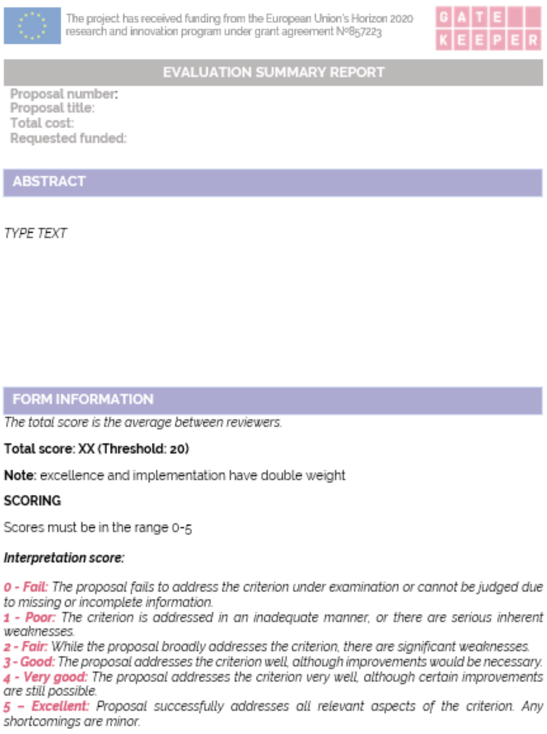
Bank name			
Branch address (full address – PO box not accepted)			
Street name and number			
Postal Code		*Town/City*	
Country			
Account no			
Bank sorting code			
International Bank Account Number (IBAN) The IBAN is mandatory for all European Partners. Where no IBAN is provided increased bank-fees are charged to the partners. See also http://www.ecbs.org/iban.htm			
BIC/SWIFT			

Requested »reason for payment« (if other than EU project name or n°) / Remarks

We certify that above information declared is complete and true.

BANK STAMP + SIGNATURE BANK REPRESENTATIVE*	DATE, STAMP + SIGNATURE of ACCOUNT HOLDER
Obligatory)	(Obligatory)

Appendix I Evaluation summary report



The project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement N°857223

EVALUATION SUMMARY REPORT

Proposal number:
Proposal title:
Total cost:
Requested funded:

ABSTRACT

TYPE TEXT

FORM INFORMATION

The total score is the average between reviewers.

Total score: XX (Threshold: 20)

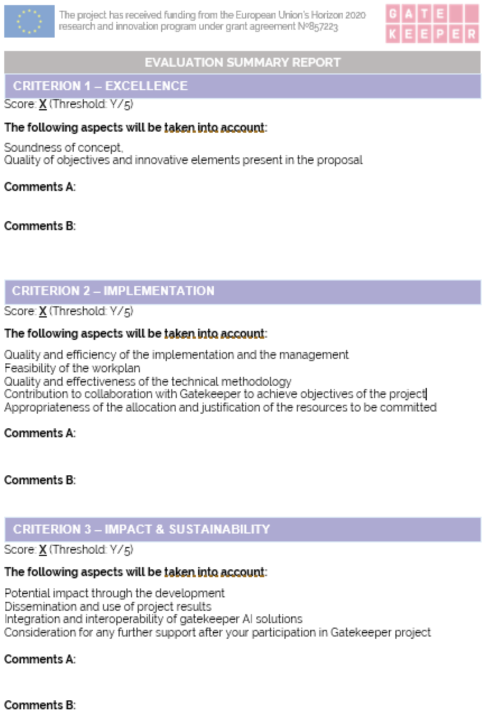
Note: excellence and implementation have double weight

SCORING

Scores must be in the range 0-5

Interpretation score:

0 - Fail: The proposal fails to address the criterion under examination or cannot be judged due to missing or incomplete information.
1 - Poor: The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.
2 - Fair: While the proposal broadly addresses the criterion, there are significant weaknesses.
3 - Good: The proposal addresses the criterion well, although improvements would be necessary.
4 - Very good: The proposal addresses the criterion very well, although certain improvements are still possible.
5 – Excellent: Proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.



The project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement N°857223

EVALUATION SUMMARY REPORT

CRITERION 1 – EXCELLENCE

Score: X (Threshold: Y/5)

The following aspects will be taken into account:

Soundness of concept,
Quality of objectives and innovative elements present in the proposal

Comments A:

Comments B:

CRITERION 2 – IMPLEMENTATION

Score: X (Threshold: Y/5)

The following aspects will be taken into account:

Quality and efficiency of the implementation and the management
Feasibility of the workplan
Quality and effectiveness of the technical methodology
Contribution to collaboration with Gatekeeper to achieve objectives of the project
Appropriateness of the allocation and justification of the resources to be committed

Comments A:

Comments B:

CRITERION 3 – IMPACT & SUSTAINABILITY

Score: X (Threshold: Y/5)

The following aspects will be taken into account:

Potential impact through the development
Dissemination and use of project results
Integration and interoperability of gatekeeper AI solutions
Consideration for any further support after your participation in Gatekeeper project

Comments A:

Comments B:

Appendix J Status performed activities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 857223

GATE KEEPER

Status of Perfomed activities

1. ACTIVITIES STATUS

1.1 Work Plan

Complete the following table that summarizes your work plan tasks defined in your proposal:

Table 19. Work plan tasks status

Work plan task	Description	Starting Month	Ending Month	Status
				Not Started/Ongoing/finished/delayed

Also, describe the status of your work plan tasks. For that purpose, for each of your planned tasks indicate the following:

- Its status. The task could be: not started, ongoing, finished or delayed.
- In the case the task has been delayed, explain why.
- Report the problems encountered and corrective measures applied.

1.2 Deliverable

Complete the following table that summarizes your deliverables (defined in your proposal):

Table 20. Deliverable status

Nº	Deliverable name	Description	Type	Delivery	Status
					Not Started/Ongoing/finished/delayed

For each of your planned deliverables indicate the following:

- Its status. It Could be: not started, ongoing, finished or delayed.
- In the case the deliverable has been delayed, explain why.
- Report of problems encountered, and corrective measures applied.

2. INTEGRATION IN THE PLATFORM

Describe the status of the integration,

- Current status:
- Plan for the next month:
- Issues:

3. DISSEMINATION and COMMUNICATION

3.1 External

In case you are disseminating and communicating the partnership, please tell us

- Name of the Event,
- Social media channel (if any)
- When

This information will help us to share it with the commission

3.2 Internal

Please let us know the internal meetings held during the current month with your mentor and other internal meetings arranged with other members of the GK consortium.

- Current meetings (month)
    - Mentor
    - Other members
- Future meetings (scheduled)
    - Mentor
    - Other members

4. HOT TOPICS

Report here the potential problems and risks you are facing. If possible, indicate your contingency and mitigation strategies.

Table 21. Detected Problems

Potential risk	Countermeasure/s
Problem 1	
Problem 2	

Table 22. Potential risk

Potential risk	Countermeasure/s
Risk 1	
Risk 2	