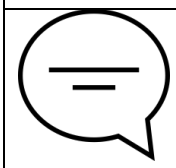
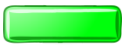
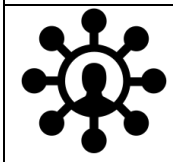
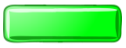
Roadmap for internet of things (IoT)

Description and state of the art	
 Definition	IoT is based on the convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems and the proliferation of smart devices. IoT stands for the internetworking of physical devices, vehicles (also referred to as "connected devices" or "smart devices"), buildings and other items – embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data[162]. IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities[163]. The Internet of Things, Industrial Internet, and Internet of Everything will gradually morph into the *Internet of Anything (IoA)*. IoA envisions a common software "ecosystem" capable of accommodating any and all sensor inputs, system states, operating conditions, and data contexts — an overarching "Internet Operating System"[164].
 Addressed societal /business or public sector need	Societal need: Inclusive well-being and health
 Existing solutions /applications /services	There are several applications of the IoT technology in the area of Health, the latter pertaining to providing assistance to people or enabling automated medication and maintenance of medical devices[165]. According to Dimitrov, "devices and mobile apps are now increasingly used and integrated with telemedicine and telehealth via the medical Internet of Things (mIoT)"[166].

 Main actors regarding R&D of this technology	• Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V. • Commissariat a l'Energie Atomique et aux Energies Alternatives • Institut National de Recherche en Informatique et en Automatique • University of Surrey • Atos Spain SA
 Current research activities	Indicative R&D projects include: • **Make it ReAAL**, a project to promote standards, guidelines and open platforms for interoperable solutions in the domain of active and independent living[167]. • **DoctorCloud**, an innovative ICT platform in the service of elder and patients for emergencies[168]. • **REMOSIS** ("Remote Mosquito Situation and Identification System"), a novel smart trap station as an Internet of Things surveillance solution to remotely count and identify the species of disease-carrying mosquitoes[169, 170]
 Impact assessment	**Public sector modernization:** • Degree of Resources (Capital, Personnel, Infrastructure) Utilization • Efficiency / Productivity • Quality of Services Provided **Public Sector as an Innovation Driver:** • Productivity (Labour / Capital / Resource) & Growth • Employment • Quality of Health • Privacy & Security • Public Safety • Transport Infrastructure • e-Security • Quality of the Biosphere • Energy Consumption – Natural Resources Utilization • Environmental Awareness Creation
Necessary technological modifications	
 Potential use cases	Potential applications of the IoT technology in the domain of health care include: • Remote health monitoring • Emergency notification systems / contacting the hospital in case of emergencies • Telemedicine • Early detection of and warning about patients at risk Dimitrov expects a new category of "personalised preventative health coaches" (Digital Health Advisors)" to emerge. He expects them to help their clients avoid chronic and diet-related illness, improve cognitive function, achieve improved mental health and achieve improved lifestyles overall[166].

 Tecnological challengehs		As for every technology, for the Internet of Things to thrive there are major technological challenges to overcome: The development of IoT networks has turned into a serious **security** concern, which derives from the fact that IoT devices are becoming more and more ingrained in our lives[171]. In fact security concerns are no longer limited to the protection of sensitive information and assets; even human lives and health can become the target of IoT hack attacks, as indicated by the hacking of pace makers[172]. **Connecting** so many devices is another big challenge for IoT that defies the very structure of current communication models. The latter are currently relying on the centralized server/client paradigm to authenticate, authorize and connect different nodes in a network and are sufficient for current IoT systems but will turn into a bottleneck when IoT networks grow to join billion of devices, thereby calling for their decentralisation[171]. IoT is growing in many different directions, with many different technologies competing to become the standard. This causes **compatibility** issues and requires the deployment of extra hardware and software when connecting devices. Additional compatibility challenges stem from non-unified cloud services, lack of standardized M2M protocols and diversities in firmware and operating systems among IoT devices. What's more they are further accompanied by **longevity** challenges, as some of the former technologies are to eventually become obsolete in the next few years, effectively rendering the devices implementing them useless.
Necessary activities (in or for the public sector)		
 Development of a specific training necessary	**Open task**	Specific training is necessary in the case of developers, which may be ignorant of the threats of IoT programming and run the risk of dishing out code that is reliable from a functionality perspective, but can easily exploited be exploited remotely[173].
 Advanced or adapted ICT infrastructure needed	**Open task**	The infrastructure needed in order to enable devices to understand their environment and act accordingly involves a combination of sensors, actuators, distributed computing power, wireless communication on the hardware side interacting with applications, and big data on the software side[173].

 Change of (public sector internal) processes necessary	**Open task**	The increased automation that is made possible by IoT calls for internal reforms in various processes, as existing manual as well as semi-automated tasks can be instantly executed thanks to the IoT advancements.
 Promotion / information of stakeholders necessary	**Open task**	Informative material on both the use and threats of IoT solutions for end users needs to be developed to support them in ensuring their privacy. This should also include information on personal and private data handling IoT devices
 Need to deal with cyber security issues	**Open task**	Security issues are data related. Health monitoring data is sensitive data and must be treated with the utmost **privacy**, as they can tell a lot about the end-user. Hence, securing the data is an open issue and must be a top priority for the success of the adoption of the particular technology.
 New or modified legislative framework or regulations necessary	**Open task**	Additions or amendments to the legislative framework are necessary as **regulations about the privacy and security of data** are to play a critical role. Attention is drawn to the fact that only in late January 2013, some relevant recommendations were provided by the Commission nationale de l'informatique et des libertés (CNIL), an administrative regulatory body whose mission is to ensure data privacy[173].
 Development of a common standard necessary	**Open task**	One of the main obstacles for a full adoption of connected devices and the Internet of Things as a consequence is the lack of standards. As long as there are no predominant standards, connected devices will not convince common users, aside from tech-savvy early adopters. To achieve maturity, the creation of a **stable market with compatible protocols** is needed. Moreover, a smooth transition from IPv4 toward IPv6 is critical for the spread of the connected devices[173]. The importance of consistency across the IoT industry is also underlined by the creation of the Global Standards Initiative on Internet of Things (IoT-GSI), which promotes a unified approach in telecommunication standardisation for the

		development of technical standards[174].
 Need for a more economical solution		There is no need for a more economical solution, as IoT devises and sensors have reached a maturity level that are cheap enough for deployment.
Dealing with challenges		
 Ethical issues		No ethical issues identified.
 Societal issues	**Open task**	Societal issues concern the **rise of unemployment** as a result of the greater dependence upon technology and the fewer requirements in human resources.
 Health issues		No health issues identified.
 Public acceptance		The technology is indeed likely to encounter problems regarding public acceptance. End-users' apprehensions about privacy and security will decide upon the success of connected devices and the Internet of Things in the area of health and well-being[173]. Further to that, the less user-friendly the products will be, the fewer customers will want to use it. With open standards, data would be simpler to share. And once the Internet of Things is as easy as an app, the adoption rate will see a boost of its adoption[173].