Symbiosis of smart objects across IoT environments

688156 - symbIoTe - H2020-ICT-2015

Final Report on Business Models and Sustainability

The symbIoTe Consortium

Intracom SA Telecom Solutions, ICOM, Greece
Sveučiliste u Zagrebu Fakultet elektrotehnike i računarstva, UNIZG-FER, Croatia
AIT Austrian Institute of Technology GmbH, AIT, Austria
Nextworks Srl, NXW, Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni, CNIT, Italy
ATOS Spain SA, ATOS, Spain
University of Vienna, Faculty of Computer Science, UNIVIE, Austria
Unidata S.p.A., UNIDATA, Italy
Sensing & Control System S.L., S&C, Spain
Fraunhofer IOSB, IOSB, Germany
Ubiwhere, Lda, UW, Portugal
VIPnet, d.o.o, VIP, Croatia
Instytut Chemii Bioorganicznej Polskiej Akademii Nauk, PSNC, Poland
NA.VI.GO. SCARL, NAVIGO, Italy
Universität Zürich, UZH, Switzerland

For more information on this document or the symbIoTe project, please contact:
Sergios Soursos, INTRACOM TELECOM, souse@intracom-telecom.com

Document Control

Title: Final Report on Business Models and Sustainability

Type: Public

Editor(s): Corinna Schmitt, Patrick Poullie, Yves Steiner, and Burkhard Stiller (UZH)

E-mail: {schmitt | poullie | stiller}@ifi.uzh.ch, yves.steiner2@uzh.ch

Author(s): Corinna Schmitt, Patrick Poullie, Yves Steiner, and Burkhard Stiller (UZH); Reinhard Herzog and Michael Jacoby (IOSB); Joao Garcia (UW); Gerhard Dünnebeil, Mario Drobics, Karl Kreiner, and Patrick Zwickl (AIT); Aleksandar Antonic (UNIZG-FER); Matteo Pardi (NXW); Sofia Aivalioti (S&C); Antonio Paradell Bondia (ATOS/WLI); Lara Lopez (ATOS); Michele Bertolacci (Navigo)

Doc ID: D1.5-v1.0

Amendment History

Version	Date	Author	Description/Comments
v0.1	Sep. 20, 2017	Corinna Schmitt (UZH)	Initial Table Of Contents
v0.2	Sep 26, 2017	Corinna Schmitt (UZH)	Content for Chapter 3, definition of sustainability and symbIoTe
v0.3	Oct 3, 2017	Patrick Poullie (UZH)	Integrated feedback received by email
v0.4	Oct 5, 2017	Patrick Poullie (UZH)	Integrated feedback from mail exchanges
v0.5	Oct 13, 2017	Patrick Poullie (UZH)	Integrated Feedback from Telco for use case Smart Mobility and ecological Routing
v0.6	Oct 24, 2017	Patrick Poullie (UZH)	Integrated Feedback from Telco for use case Smart Residence
v0.7	Oct 31, 2017	Patrick Poullie (UZH)	Integrated feedback received by email
v0.8	Nov 1, 2017	Patrick Poullie (UZH)	Pre-final version to request comments from all
v0.9	Dec 1, 2017	Patrick Poullie (UZH)	Integrated feedback from Zagreb meeting
v0.10	Dec 7, 2017	Corinna Schmitt, Patrick Poullie (UZH)	Finalized Sections on Tussle Analysis (TA) and applied new Template
v0.11	Dec 8, 2017	Patrick Poullie (UZH)	Minor corrections in TA sections
v0.12	Mar 4, 2018	Corinna Schmitt (UZH)	Minor corrections in IoT Ecosystems analysis section
v013	Mar 5, 2018	Corinna Schmitt (UZH)	Input on CANVAS section for UC Smart Residence
v0.14	Mar 11, 2018	Corinna Schmitt (UZH), Matteo Pardi (NXW)	Final comments addressed for CANVAS UC Smart Residence
v0.15	Mar 12, 2018	Corinna Schmitt (UZH)	Input on CANVAS section for UC EduCampus
v0.16	Mar 13, 2018	Corinna Schmitt (UZH)	Added third show-case for UC Smart Residence
v0.17	Mar 13, 2018	Corinna Schmitt (UZH), Sofia Aivalioti (S&C), Karl Kreiner (AIT)	Added final feedback to CANVAS Healthy Indoor Air and AAL
v0.18	Mar 20, 2018	Corinna Schmitt (UZH), Karl Kreiner (AIT), Reinhard Herzog (ISOB)	Added feedback to CANVAS AAL and final feedback for CANVAS EduCampus
v0.19	Mar 21, 2018	Corinna Schmitt and Yves Steiner (UZH), Karl Kreiner (AIT)	Added final feedback to CANVAS AAL, Included current graphs to VNAs
v0.20	Mar 22, 2018	Corinna Schmitt (UZH)	Added CANVAS for UC Smart Mobility and Ecol. Routing
v0.21	Mar 26, 2018	Corinna Schmitt (UZH), Joao Garcia (UW)	Added CANVAS feedback for UC Smart Mobility and Ecol. Routing, Input on CANVAS section for UC Smart Yachting
v0.22	Apr 11, 2018	Corinna Schmitt (UZH), Aleksandar Antonic (UNIFER)	Addressing Comments to CANVAS UC Smart Mobility
v0.23	Apr 12, 2018	Corinna Schmitt (UZH), Michele	CANVAS UC Smart Yachting added show-case description, Text

		Bertolacci (Navigo)	creation for CANVAS content
v0.24	Apr 18, 2018	Corinna Schmitt (UZH), Michele Bertolacci (Navigo)	CANVAS UC Smart Yachting added show-case description, Text creation for CANVAS content
v0.25	Apr 19, 2018	Yves Steiner (UZH)	VNA UC EduCampus description and replacement of VNA graphics with latest versions.
v0.26	Apr 24, 2018	Corinna Schmitt (UZH), Lara Lopez (ATOS)	CANVAS UC Smart Stadium
v0.27	Apr 24, 2018	Corinna Schmitt (UZH)	Harmonize CANVAS Figures
v0.28	Apr 24, 2018	Corinna Schmitt (UZH), Lara Lopez (ATOS)	CANVAS UC Smart Stadium final text and agreement
v0.29	Apr 25, 2018	Corinna Schmitt (UZH)	GDPR description started
v0.30	Apr 26, 2018	Yves Steiner (UZH)	VNA Theory
v0.31	May 6, 2018	Corinna Schmitt (UZH)	GDPR description completed
v0.32	May 14, 2018	Corinna Schmitt (UZH)	Abbreviations added
v0.33	May 14, 2018	Corinna Schmitt (UZH)	Executive summary, Introduction, Definition, Document Structure, Conclusion added initially
v0.34	May 28, 2018	Yves Steiner (UZH)	Including all VNA, business model and sustainability sections.
v0.35	May 30, 2018	Yves Steiner (UZH)	Updating VNA, business model and sustainability
v0.36	June 1, 2018	Corinna Schmitt (UZH)	Finalization of sections before submitting to internal review
v0.37	June 4, 2018	Reinhard Herzog (IOSB), Gerhard Dünnebeil (AIT)	Internal Reviews
v0.38	June 6, 2018	Corinna Schmitt (UZH)	Addressing internal review comments
v0.39	June 18, 2018	Burkhard Stiller (UZH)	Final checks
v1.0	June 21, 2018	Sergios Soursos (ICOM)	Minor editorial changes

Table of Contents

(This page is left blank intentionally.)

1 Executive Summary

The Deliverable D1.5 presents a business model recommendation for symbIoTe including items for sustainability. Upon starting the IoT-ecosystem is analyzed leading to the impression of a fragmented situation in the current IoT domain, especially at data collection opportunities and applications using the data collected. Involved standards and services from collection points up to the application presenting the data are highly diverted. This fragmentation is also obvious when analyzing the stakeholders involved in the IoT. They can be grouped in different ways, but clearly have a concrete and well-defined own view of IoT individual incentives. All these facts make up for a good motivation for a solution like symbIoTe to overcome the current fragmented situation.

Therefore, symbIoTe specifies five use-cases covering typical application areas in today's IoT and offers especially interoperability, security, and smart spaces. In order to develop a promising business model recommendation three different methods were applied to each use-case, namely CANVAS, Tussle Analysis, and Value-Network-Analysis. All three methods together investigate the Business-to-Business (B2) and Business-to-Customer (B2C) relationship to identify requirements, benefits, and incentives for stakeholders involved. As a result, needs are specified that have to be addressed by software and hardware, as well as from the finance sector. The investigations show that some global requirements and necessities can be agreed upon for all use-cases (e.g., cost structure or revenue streams), however particular findings are very specific to the individual use case. Thus, only use-case specific recommendations for a business model are possible and sensible. This also holds for sustainability items that are highly influenced by stakeholder requests (e.g., reducing times, increase quality of service, or reducing cost).

Summarizing, symbIoTe offers an excellent service variety to overcome the fragmented situation of today's IoT domains, addressing many concerns and wishes of users and at the same time providing a component-based solution applicable to many different scenarios in IoT. The recommended business model is similar to existing ones, but weight issues differently based on the use-case. This means different offerings are in focus depending on the infrastructure used and the audience target. To bring successfully a solution to the market the ecosystem must be analyzed continuously and the current business model must be adapted to the solution.

2 Introduction

This deliverable D1.5 presents the business model recommendation and sustainability plan for symbIoTe. In the early stage of preparation, it became obvious that the use-cases considered show high diversity, not only from stakeholders involved and key resources, but also with respect to the target audience. Furthermore, it could be recognized that from a business perspective two views need to be analyzed with individual weights:

1. Business-to-Customer (B2C) perspective
2. Business-to-Business (B2B) perspective

In some use-cases (e.g., Smart Stadium or Smart Residence) also a combination of these two perspectives must be considered for the business model. Due to these aspects, it was concluded to be more efficient to develop use-case specific recommendations and mention common aspects at the end of each development.

To build such recommendations an ecosystem analysis was required in the beginning, proving the diversity of the IoT landscape and the complexity of stakeholders having different incentives for their involvement. Further different business models are on the market and are applied in a use-case specific manner.

In a next step, dedicated methods were selected and applied sequentially to determine the recommendation at objective grounds. Each method's output was used in combination with other deliverables' content and internal discussions as input for the next method (cf. Figure 1). The methods used include CANVAS, Tussle Analysis, and Value-Network-Analysis, all described in detail in Section 4.1.

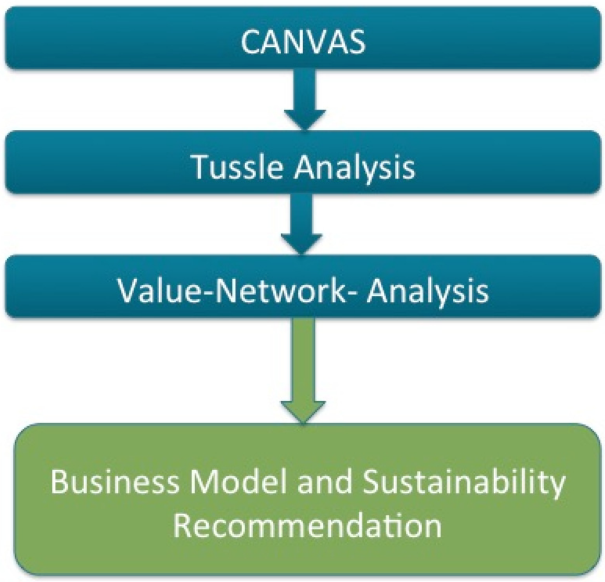

Figure 1: Workflow toward business model and sustainability

The output of Chapter 4 is used to develop final recommendations for each individual use case. The recommendations – as presented within chapter 5 – address business models and sustainability aspects. Additionally, they highlight strategies common to all use cases.

2.1 Purpose of this Document and Relation to Other Deliverables

The purpose of this deliverable D1.5 is to present the state-of-the art analysis of the IoT Ecosystem identifying (1) the complexity of the market structure, especially the diversity of stakeholders and (2) relevant business models currently in place on the market. Having this in mind, this deliverable indicates a business model recommendation and sustainability plan for symbIoTe. Therefore, different methods were applied by looking on each use-case from a Business-to-Customer (B2C) and Business-to-Business (B2B) perspective. Overall, some similarities for the business model recommendation and sustainability can be identified, but due to the larger use-case diversity many differences exist.

The deliverable D1.5 especially uses the following deliverables as input:

- D1.3 – Final Specification of Use Cases and Initial Report on Business Models [15]
- D5.2 – Report on System Integration and Application Implementation [35]

The content of deliverable D1.5 is used mainly by two work packages and their upcoming deliverables:

- WP7 for the exploitation plan
- WP5 for the upcoming use-case based trials and deployments

2.2 Terminology and Definitions

As stated in D1.3 [15] the IoT ecosystem is highly fragmented today, facing an increasing number of new IoT platforms on the market and a request for interoperability. This request is addressed by symbIoTe. Thus, symbIoTe is defined as a viable interoperability framework enabling platform collaboration and cooperation.

Stakeholders can be manifold as already stated in D1.4 [55]. The following list shows the main definitions of different stakeholders the symbIoTe consortium agreed on in previous deliverables:

- **IoT Platform Provider** offers IoT services managed by an IoT platform (reside within symbIoTe Cloud Domain).
- **Application Developer** builds IoT applications based on the IoT services exposed by various IoT platforms (reside at the symbIoTe Application Domain).
- **End User** is an individual user of a symbIoTe-supported IoT application.
- **Infrastructure Provider** physically deploys the necessary hardware and software infrastructure within smart spaces.
- **Prosumer** (e.g., platform or end user) is a stakeholder who at the same time produces/provides resources/goods, but also consumes resources/goods provided by other producers or prosumers.
- **Consumer** does not provide any resources/goods and can participate only in trading transactions, which allow him/her to gain access to resources registered within the symbIoTe Core Services.
- **Producer** provides resources/goods within the symbIoTe ecosystem and can engage in trading and bartering transactions.

During the preparation of this deliverable many discussions took place in order to map the stakeholders named within each use case into the aforementioned stakeholder definitions.

Depending on the dedicated use-case under consideration such as mapping is very hard, sometimes impossible, since many examples can be found, where a stakeholder can be a consumer/end user and prosumer at the same time. Similar situation occur while looking on developers and providers. Thus, it was decided by the use-case owners to use the following definition for a stakeholder, which is applied within D1.5:

"A stakeholder is a role. This role can be impersonated by individuals, legal bodies, things, or software."

2.3 Document Structure

Chapter 3 presents the state-of-the-art analysis of the current ecosystem of IoT indicating the layered structure of the IoT domain. Further, this section presents different grouping possibilities of stakeholders based on their purpose and incentives showing the high diversity in today's IoT. This diversity can also be found in finance strategies applied in IoT.

Chapter 4 introduces three different methods to build a business model recommendation and to identify sustainability items for symbIoTe. The CANVAS method investigated different building blocks (e.g., relationships, target audience, activities, cost structure, and revenue stream) focusing mainly on the Business-to-Customer (B2C) perspective. Stakeholders are influenced from related solutions coming newly onto the market. Such influences might be interfering or beneficial. The Tussle Analysis identifies the effects of such influences. While these methods address the Business-to-Customer perspective, a bit of the the Business-to-Business (B2B) relationship is relevant, too. However, the latter is mainly addressed by the Value-Network-Analysis performed, clearly identifying the values exchanged and listing the benefits and incentives for all stakeholders involved. Those three methods are applied to each symbIoTe use-case as they require a specific description and a well defined use-case. Each result is used as an input for the subsequent method.

Chapter 5 specifies the individual business model recommendation and sustainability items for each use-case as a result from Chapter 4. As it can be seen, selected items might be similar for the use-cases, but also a larger diversity is in place.

Finally, Chapter 6 concludes the deliverable summarizing Chapters 2 to 4 with their main aspects and findings.

3 State of the Art Analysis

In the Internet of Things (IoT) paradigm, objects that people use to manage, monitor, and optimize the operational aspects of their daily activities are no longer unresponsive devices. Instead, they are interactive devices connected to the Internet with intelligence and many more capabilities (such as sensing, communication, processing, and storage) [1, 2]. However, privacy attacks and harmful consequences can occur when sensitive information is concealed or controlled without users' consent [2]. Because of application interdependency and data sensitivity, a small leakage of information could severely damage user privacy. Further, users will accept IoT deployments only if the infrastructures are secure, trustworthy, and privacy-preserving.

Because IoT comprises heterogeneous networking technologies and devices, such as radio frequency identification (RFID) tags, smartphones, and sensors, it is challenging to deploy conventional privacy protocols, as high-performing devices sometimes require advanced protocols that are too bulky for these small devices. However, lightweight privacy solutions are easily tractable by powerful attackers [2]. [18-20]

Cisco estimates that by 2020 there will be more than 50 billion Web-enabled devices, including refrigerators, televisions, and scales [12]. Internet and cloud service providers (ISPs and CSPs) and consumers have already encountered many global privacy threats due to the use of pervasive products and services. Recent press reports highlight several privacy violations in IoT applications [4, 5]. For example, in June 2013, the press revealed privacy risks related to the Planning Tool for Resource Integration, Synchronization, and Management (PRISM) program, which the US National Security Agency uses to collect private electronic data belonging to users of major Internet services including Microsoft Outlook, Google, and Facebook. Further, an annual Internet security threat report claims that mobile malware attacks increased by 58 percent from 2011 to 2012, and 32% of those attacks attempted to steal information from the device's contact information. According to a US Federal Trade Commission (FTC) report on consumer privacy, Privacy–by-Design (PbD) is the most prominent approach to overcoming IoT privacy issues [6]. [18-20]

3.1 IoT Ecosystem Analysis

A business ecosystem is the community of business entities that is formed by the competitive and collaborative interactions among business entities for innovations. A business ecosystem evolves to form a new value network, and thus, to create a new market. The IoT domain has various applications including, smart home, connected car, connected health, and business/industrial applications. Thus, many business players across diverse industries including semiconductor, consumer electronics, IT (Internet Technology), telecom, healthcare, medical devices, retail, industrial & manufacturing and transportation are participated in the IoT business ecosystem[1]. According to Research and Markets, there are more than 2000 companies that are selling IoT enabled products, playing a vital role in the IoT technology innovation, or act as an enabler to the IoT business development.

[1] https://www.semiwiki.com/forum/content/5338-internet-things-2015-year-end-review-iot-business-ecosystem.html (last visit May 14, 2018)

Deloitte published a report on the IoT Ecosystem in 2014 pointing out the following characteristics of the IoT [22]:

- "The IoT has the potential to offer business value that goes beyond operational cost savings. "
- "Providers in the IoT ecosystem have a largely unexplored opportunity to develop compelling IoT solutions that explore how the ability to collect and analyze disparate data, in real-time and across time, might transform the business. "
- "These developments will play out within and across enterprises, offering opportunities for sustained value creation and even disruption for those who can imagine possibilities beyond the incremental."

In the following the IoT ecosystem is investigated based on existing literature. First, in Section 3.1.1 the layered architecture of IoT is introduced with the purpose to understand the diversity in place from a common view based on [18-20]. This is followed by a detailed analysis of the IoT ecosystems from the view of stakeholders [22].

3.1.1 Layered Representation of IoT Technologies

The continuous evolution of the IoT architecture and the complexity of its underlying technologies, as well as the many visionaries involved in its development, make it difficult to define with sharp boundaries [1,3]. A horizontal representation of IoT driver technologies illustrates the connectivity and common operational platforms (cf. Figure 2). The functionalities of the layers are defined with respect to the Open Systems Interconnection (OSI) model layers.

The *edge network layer*, which corresponds to the OSI model's physical layer, is the data perception layer, which is responsible for sensing the physical environment, collecting real-time data, and reconstructing a general perception of the data. These technologies and devices typically have short-range communication, constrained batteries, and low storage and computational power.

The *access network layer* represents the data link layer and has heterogeneous communication technologies that enable the first stage of data transmission in terms of communication path handling and data publishing. This layer's major services include message routing, publishing, and subscribing.

The *core network layer* relates to the OSI network layer and consists of the conventional Internet Protocol and Multiprotocol Label Switching (IP/ MPLS). This layer is also responsible for processing networking data and billing, as well as managing data, maintaining quality of service, supporting visualization, and enabling network security. The *service and middleware layer* resembles the OSI model's transport, session, and presentation layers. This layer abstracts and then forwards the various data formats, technologies, and communication protocols of the lower layers. It also provides data management, data filtering, data aggregation, semantic analysis, and information utilization through the management servers that facilitate cloud computing and data mining technologies.

On top of it all, the *application layer*, like the application layer in the OSI model, represents the various purposes of IoT technologies from local, national, and industrial perspectives. The ultimate goal is to ensure the usability of IoT applications with low complexity and high credibility. [18-20]

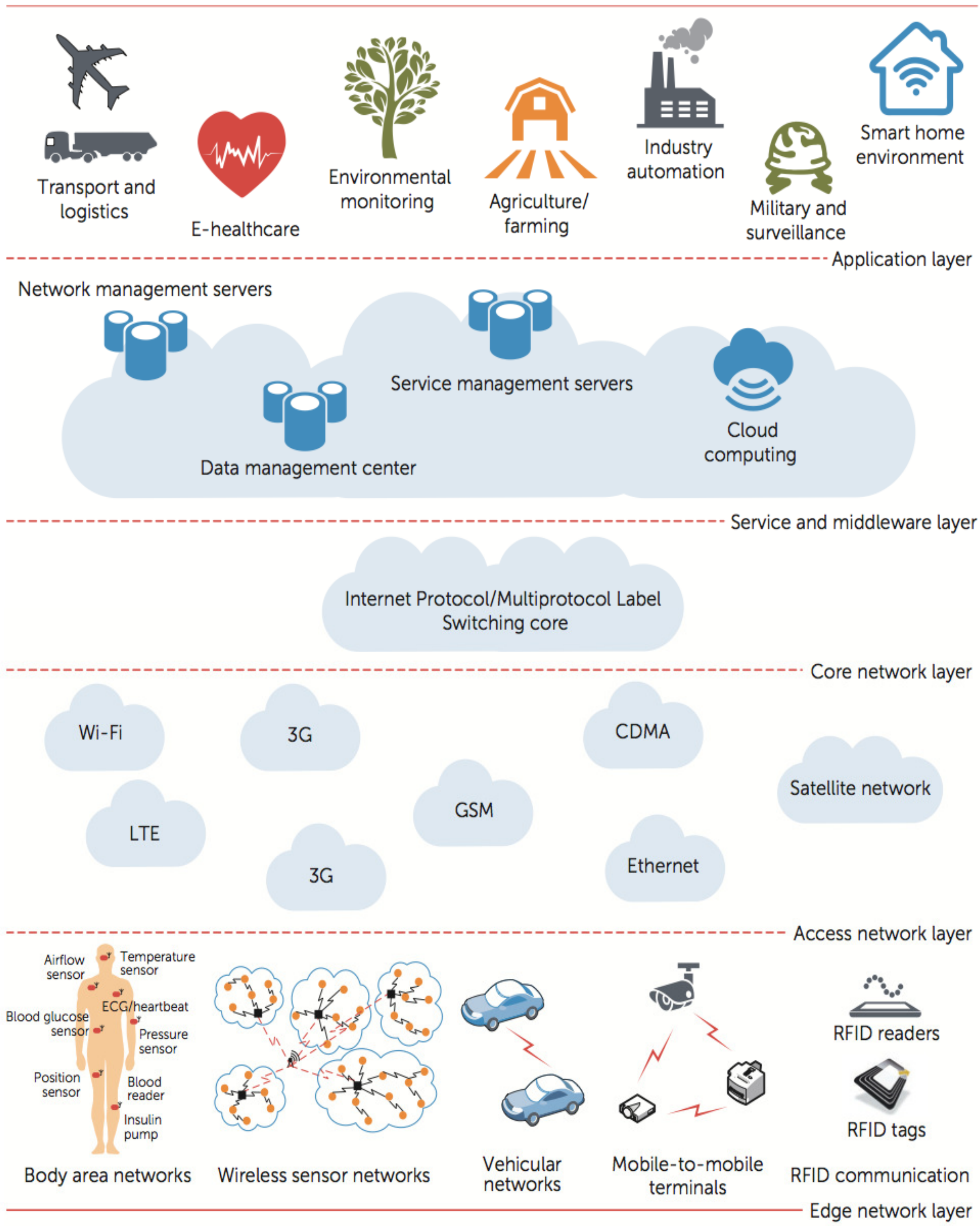

Figure 2: Horizontal representation of IoT driver technologies [18-20]

3.1.2 IoT Ecosystem – Stakeholder View

The IoT landscape became more and more complex over the years building an IoT ecosystem itself, where high diversity of stakeholders is present. Those stakeholders have different expectations on the IoT market, IoT technology, IoT architecture, and functionality, as well as their integration in the layered architecture of it. In the following the main outcomes of Deloitte's study (2014) [22], McKinsey's statement (2014), CompTIA's study (2014), and Matt Truck's study (2016) [23] are presented. Other available studies on IoT ecosystem refer to those four aforementioned once and, thus, they were selected to show the complexity of the IoT ecosystem here.

IoT Ecosystem – Deloitte View

A very high-level view was presented by Deloitte's study in early 2014 by grouping involved stakeholders based on an investigation of existing platforms and solutions on the IoT market – customers, providers, manufacturers, and vendors [22]. The mentioned solutions observed were drivers in their complexity – ranging from simple solutions involving data collection and publishing using third parties' services (e.g., Xively) to complex solutions involving many different stakeholders collecting data and offering them via a platform to other stakeholders with different purposes (e.g., HAV system company, security service, eHealth). Five groups (cf. Figure 3 [22]) of stakeholders were identified fulfilling different tasks and/or potentially influenced each other in different ways directly or indirectly, having the same global goal to simplify life and meeting the business objective of revenue streams (e.g., money benefits, new customer segments):

- The first group is presented by the customers defining what they inquire from IoT stakeholders such as special Apps and IoT services. Further, customers indicate what they are willing to pay more for the offerings. This group of stakeholders has an outstanding position compared to the following four groups building a network, because they actively influence all of them throughout the IoT landscape. Especially they define what features a product must offer to be accepted by the customers and result in financial benefits for those four groups.
- The second group represents the providers offering requested services to answer the customer's requests and charging the vendors of offered services (e.g., Cloud storage usage) for their special IoT in order to lower the fees for the customers.
- The manufactures developing required IoT devices (e.g., smart watches, smart sensors) represent the third group identified. They address the customer's service requests from a technology perspective.
- The most complex group is represented by the vendors. They develop specialized IoT services and software, specify IoT equipment and sell everything to the customers. They may request fees for that from providers and customers, and further request feedback to improve their solutions. Depending on their working area, vendors might also function as an intermediate or relay between data collection points and final user of the data (e.g., insurance, security company, power company).
- The last group identified has a complete different intention as the other four groups and condenses stakeholders with special and influencing purpose such as standardization organs and consumer protection companies. Those interest groups develop standards for different levels of the layered architecture (e.g., communication standards and security protocols), protect consumer interest (e.g., privacy support, regulation on data storage and data exchange), and influence hardware and software design for specialized services (e.g., logistics automotive, eHealth area).

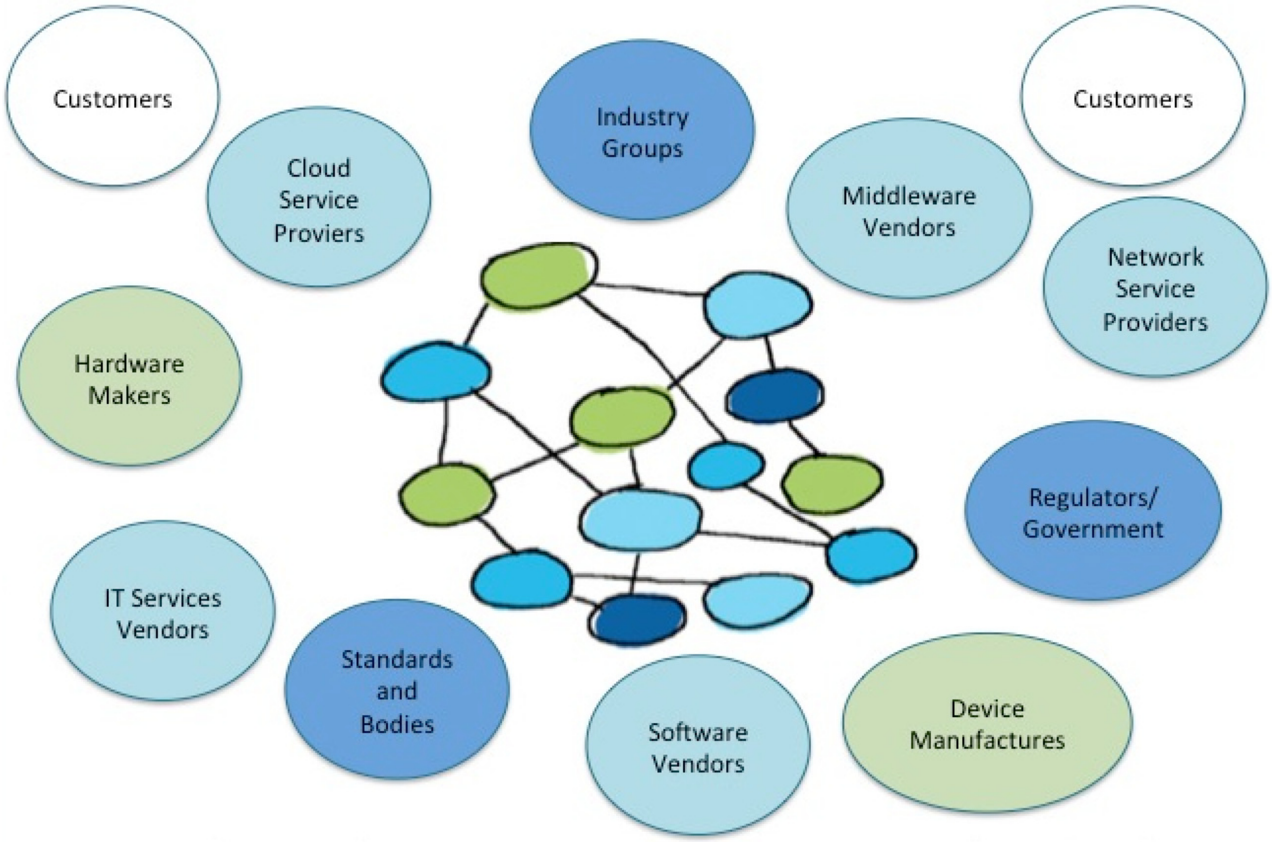

Figure 3: Stakeholder of today's IoT ecosystem [22]

IoT Ecosystem – CompTIA View

More complex IoT ecosystem analyses are also published with different scopes having the following statement from a McKinsey report[2] of 2014 in mind [14]: "...the digital technologies underlying these competitive thrusts may not be new, but they are being used to new effect." In comparison to the aforementioned Deloitte study from 2014, CompTIA[3] distinguishes in its report between hardware, software/connectivity, rules and services as work pieces that together create an IoT ecosystem inspired by stakeholders [15].

The first work item in the CompTIA report is the *hardware* summarizing all things in the IoT including sensors and commuting components that can affordably be placed in any type of device that can be produced with low costs. Additionally, miniaturizations play a big role offering data processing and sending already on the same chip without involvement of external hardware. The device diversity and supported functionality can be manifold ranging from complex systems like cards carrying over 200 sensors to very small devices such as micro motes of a size less than a cubic millimeter. Hardware on its own has a limit of use by purpose and needs support by the second piece of work – the *software*. It links everything, makes the data usable, and connects entire systems in order to share information or to communicate with the outside. Depending on hardware resources, the

[2] http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/strategic-principles-for-competing-in-the-digital-age (last visit May 14, 2018)
[3] https://www.comptia.org/resources/sizing-up-the-internet-of-things (last visit May 14, 2018)

software can be simple or complex. The complexity level is highly influenced by the different applications and available solutions for communication (e.g., cellular and Wi-Fi networks). The aforementioned two components – hardware and software – make up the technical foundation for IoT, but require a third element dedicating the way a technology develops and becomes acceptable on the market. This third element summarizes *standards, regulations, and best practice* shaping the way of development. It involves to help building rules and recommendations for the IoT ecosystem. Looking on the layered architecture of the IoT shown in Figure 2 this work item influences every layer and includes manifold stakeholders with similar or different intentions. For completeness, *services* should be mentioned as the fourth building part, combining the other three elements in a cohesive offering or to simplify the solution for the end user.

IoT Ecosystem – Matt Turck's View

Building onto the findings of CompTIA's report from 2015 a more detailed view was published in 2016 by Matt Turck, who splits the four working items mentioned above further by looking into deeper interests and announcing of big players in the corresponding areas combined with the grouping presented in Deloitte's report and the layered architecture of the IoT itself [23]. The latter breaks down the stakeholder groups into three big areas:

1. The *"application related*" area (cf. Figure 5) deals with big players in this area. One example group is built by stakeholders focusing on personal applications (e.g., wearables, fitness, health, sports, toys and elderly items). Another area is built by enterprise applications such as healthcare, retail, payments and loyalty, smart office, agriculture or infrastructure. Looking in more technical areas it would be a vehicle or the industrial Internet area.
2. The "*platform and enablement related*" field (cf. Figure 4) include stakeholders involved in the area of platforms, interfaces, 3D, etc.
3. The domain called "*building blocks*" (cf. Figure 6) summarizes the stakeholders active in the subgroups hardware, software, connectivity, and function as partners.

3.1.3 Findings

Based on the aforementioned IoT Ecosystems (Deloitte, CompTIA, and Matt Turck) in Section 3.1.2 it is obvious that today's IoT ecosystems are a combination of different areas that all have different stakeholders and solutions in place. Those can be summarized as follows represented throughout the consortium itself, open call winners from first and second rounf, customers of partners, and IoT-EPI community:

- **Users:** Mobile revolution, social & business networks, personalized and location based services
- **Enterprises:** Efficiency and end-to-end support in production process, decision taking in real-time, Big Data
- **Smart Things:** Ubiquitous communication (e.g., GSM, WiFi, BT, ZigBee, NFC), low hardware cost and high performance, software-wise embedded solutions
- **Partners:** Value-Chain optimization and flexible supply chain, real-time integration, mobility support (e.g., tracking, monitoring)

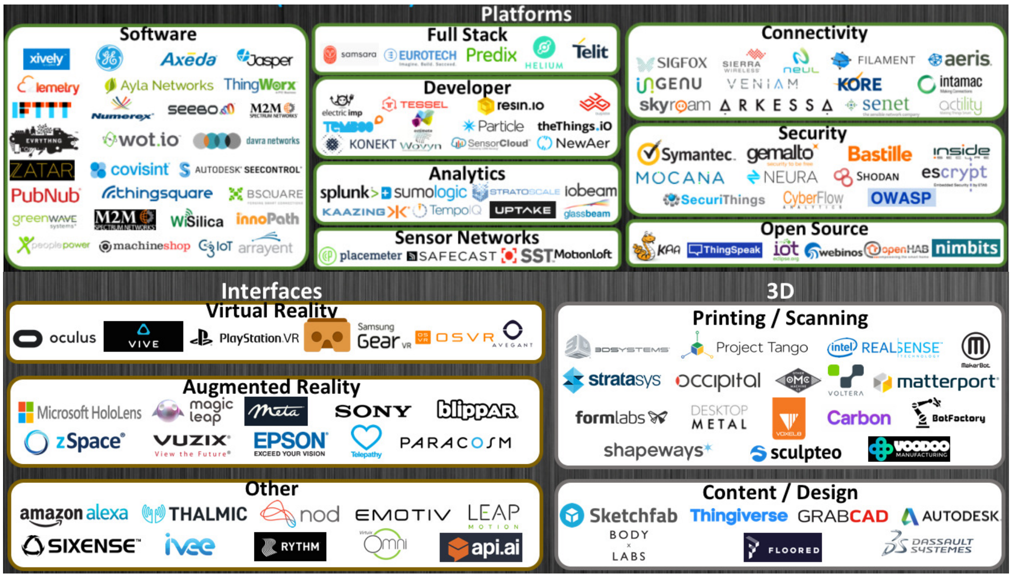

Figure 4: Stakeholders in the area „Platforms and Enablement“ [23]

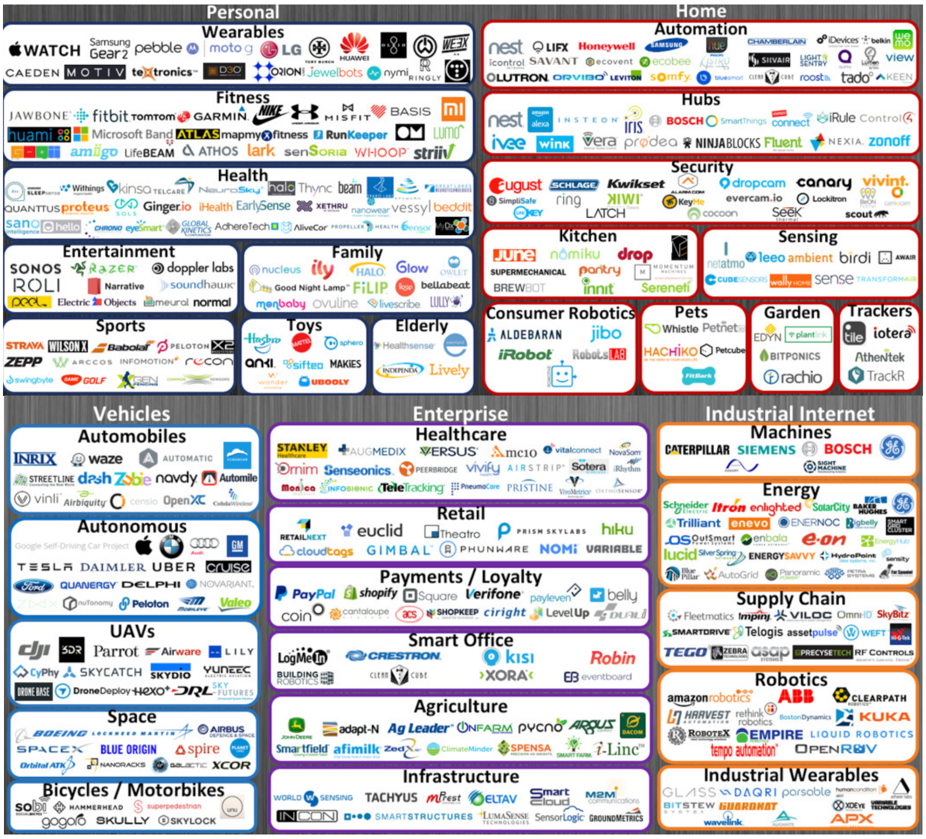

Figure 5: Stakeholders in the area „Applications“ [23]

Figure 6: Stakeholders in the area „Building Blocks“ [23]

Similar connections are shown in the following Figure 7, highlighting the different data flows in today's IoT Ecosystem in general.

Mapping the experiences shown in Figure 7 identified by Forbes in 2014 to symbIoTe's developed concept a similar inter-layer data flow becomes obvious as shown in Figure 8. The data flow is a circle that influences each other and data is flowing from top to bottom and other way round. Sensors and actuators are responsible for data and observation, they distribute the data down to analyze and visualize entities as well as to control and manage entities using gateways, interfaces, and APIs. Depending on the situation the data is further distributed to cloud solutions (e.g., storage, analysis center). When the data traveled down the layers a reaction follows based on the results causing controlling processes and gaining insights influencing sensors and actuators again. Then the circle starts again.

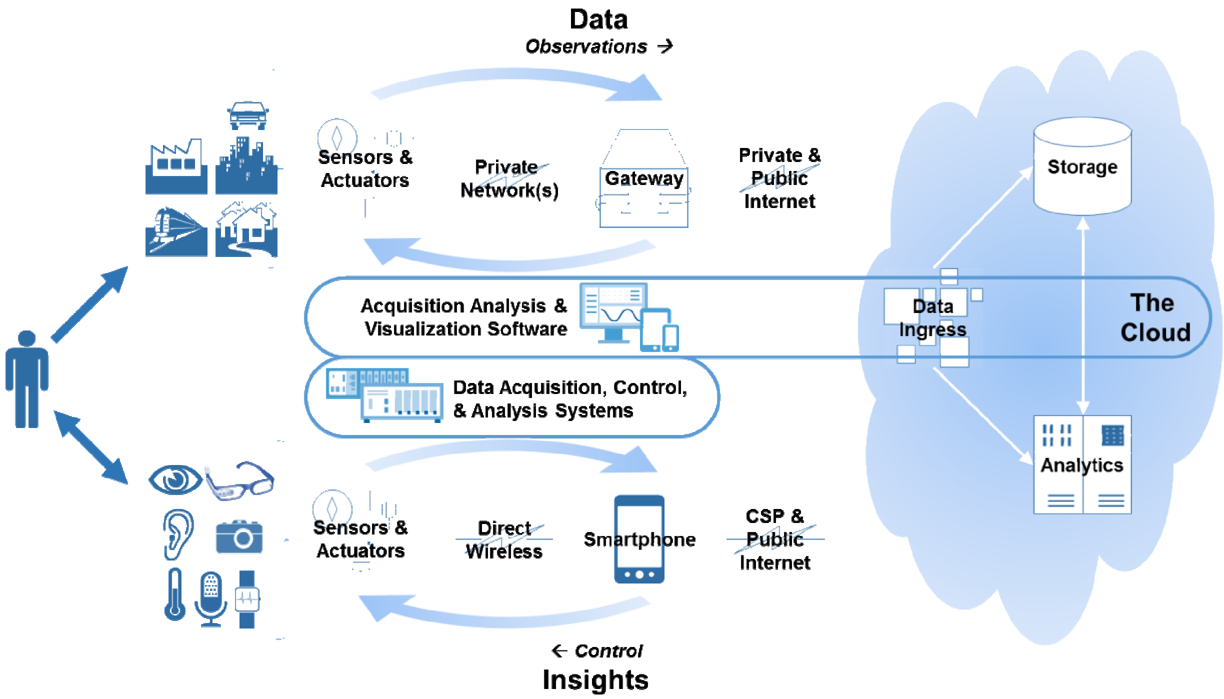

Figure 7: IoT Chain[4]

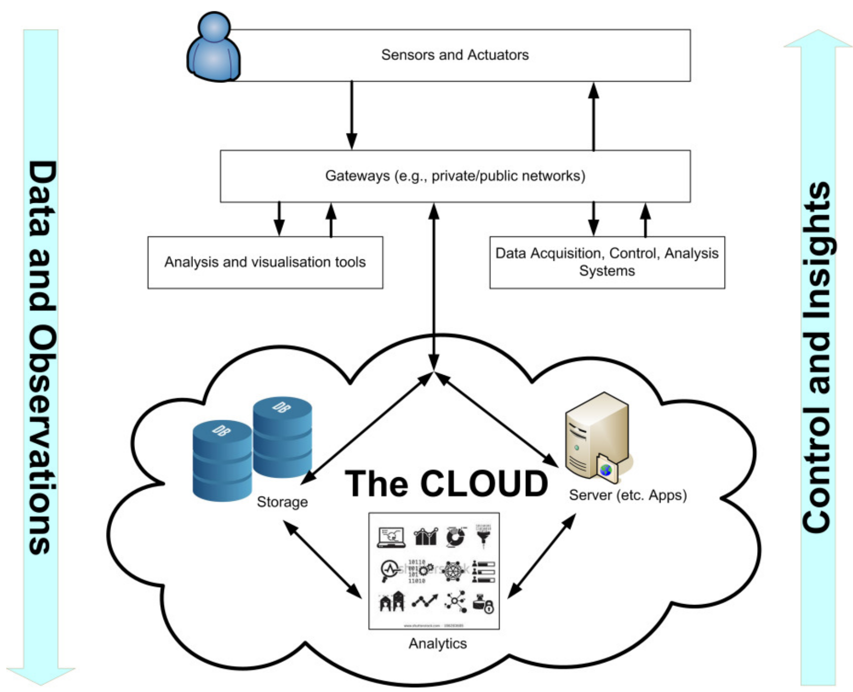

Figure 8: IoT Chain for symbIoTe showing data flow between components

[4] https://www.forbes.com/sites/patrickmoorhead/2014/11/06/national-instruments-to-enable-next-generation-design-and-test-tools-for-the-internet-of-things/#5195e9be2bfc (last visit April 19, 2018)

3.2 Technical Perspective of IoT Market Analysis

As it can easily be depicted from the layering structure shown in Figure 2 when doing a state-of-the-Art analysis, different dimensions must be investigated, depending from which viewing angle the situation is investigated. The viewing angle can depend on the mentioned layers or also coming from stakeholder perspectives and their requests. The following section gives a snapshot view on current situation.

3.2.1 High-Level Findings

Investigating different existing IoT solutions and platforms on the market, it can be recognized that those are very specific solutions:

- Technology depended, requiring special hardware and infrastructure
- Application driven based on area of expertise (e.g., eHealth, automation)
- Service-oriented with special focus on individual stakeholder requests

Those solutions and supported devices can be classified based on their intelligence and range from autonomic devices and intelligent devices (e.g., robots, actors, alarm and control systems) over dump devices (e.g., RFID-Tag, light sensors) and smart devices (e.g., wearables, smartphones) to embedded devices (e.g., in fridge, machines, cars) [3]. Nevertheless, in the taxonomy existing IoT middleware and frameworks also need to be taken into account to receive a complete view. And on the other hand, the taxonomy includes communication patterns including request/response, multicast, event subscription, active/asynchronous/reliable messaging, publish/subscribe, queues, message brokers, federation, discovery, and delegation [7]. These communication patterns can be separated into the following groups [8]:

- Human-to-Machine (H2M) communication means a human interacts with a device (e.g., interfaces, wearables).
- Machine-to-Analytic (M2A) communication means that when devices and machines monitor something (e.g., environment, personal health), it typically requires one to take a look at sensor information, analyze and interpret them.
- Machine-to-Machine (M2M) communication means one machine triggers another machine (e.g., alarm clock starts coffee machine, wireless price tag).
- Machine-to-Data-Lake (M2D) communication means machines collecting a ton of data, capture and store them for future use.
- Machine-to-Process (M2P) communication means machines can communicate directly with business processes and trigger their output and performance.
- Machine-to-Human (M2H) communication means a device speaks to humans (e.g., app informs human about packet delivery status, security system informs human about alarms).

Independent of the aforementioned findings it can be stated that each solution has to deal with technology (strongly related to privacy issues) and legal challenges as shown in Figure 9: User, Data mining, underlying technology, and legal regulations.

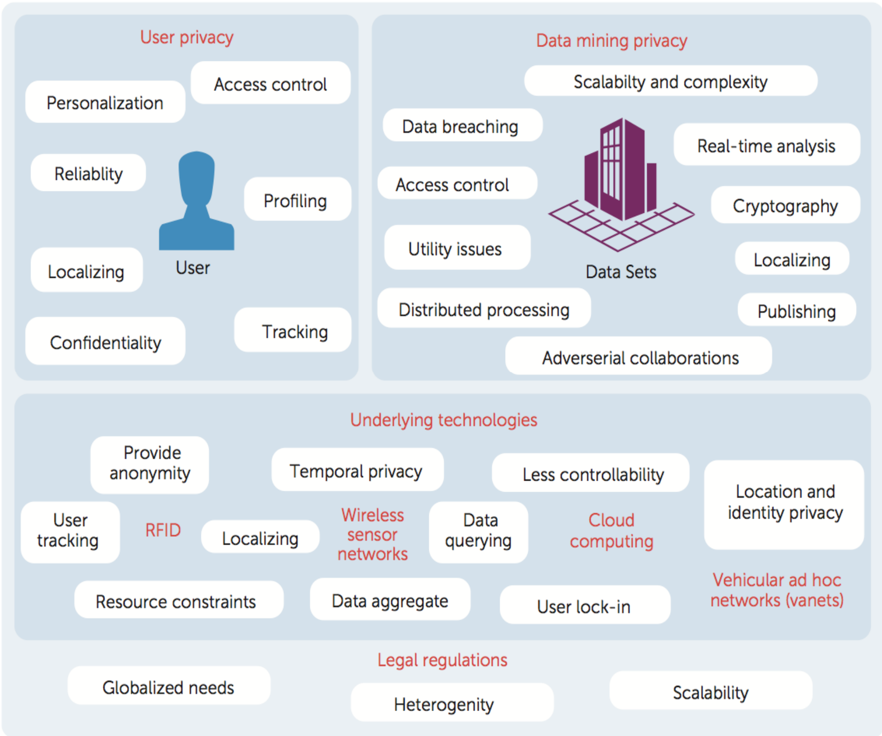

Figure 9: Technology and legal challenges in IoT [18-20]

User Privacy [18-20]

One serious user privacy issue is the identification of personal information during transmission over the Internet [2, 7]. Let's say, for example, a consumer named Bob buys an RFID-tagged object with his credit card. In some situations, Bob's personal information could be automatically linked to the object and known to the CSP. Such user information leakage can lead to privacy threats in terms of tracking, localizing, and personalization. Similarly, let's assume Bob possesses a set of objects that are linked together. If adversaries can distinguish ownership of certain objects, they might be able to estimate the ownership of the remaining objects.

These types of scenarios allow user profiling and tracking. Smartphones and other mobile devices connected to the Internet could disclose the user's geographic location and compromise privacy. In practice, users have different levels of privacy awareness and concern, and thus are ready to disclose information at different levels.

In general, IoT users might encounter privacy threats in terms of tracking, profiling, access control and confidentiality, data protection, content confidentiality and reliability, and privacy detection. Because of the IoT's range, manifold privacy risks and challenges must be considered before deploying an application or solution.

DataMining [18-20]

According to Charu Aggarwal and his colleagues, three critical enablers of IoT privacy from a data-centric perspective are scalability, distributed processing, and real-time analytics [9]. Other privacy issues they identified in this area relate to data publishing, the context of applications, utility issues, cryptography, and adversarial collaboration [9]. Scalability matters for IoT applications that contain numerous smart objects or that manage biometric data that must be collected, processed, stored, and published in large volumes of real-time, highly distributed data. Distributed processing can also lead to unprecedented challenges related to data mining privacy, along with liability for data breaches (that is, the release of secure information to distrustful entities) and distinct levels of data quality. Privacy threats related to data sharing and transmitting arise with the disclosure of location and temporally sensitive data traffic. While collecting large sets of raw data, it is challenging to balance the privacy preservation in data cleaning and the intentional reduction of data quality and original purpose without losing information needed for data mining and analysis. Collecting, sharing, and transmitting sensitive data connected to humans are the most critical privacy issues in the context of applications. Computational and theoretical limitations can be associated with privacy preservation over high-dimensional datasets. Because individuals and cooperative users have different privacy constraints, the records in a given dataset should be treated differently for anonymization purposes. The collected data might be used and published for purposes other than the original objective without user con- sent. Access control and maintenance of such data, with the assurance of privacy protection for the corresponding data owner should be carefully considered. Because computer storage mediums can store large volumes of data, they offer high availability at low cost. Consequently, once information is generated, it's most likely stored infinitely, and thus "digital forgetting" can lead to privacy violations from the data owners' perspective. [1]

Underlying IoT Technologies [18-20]

The incorporation of RFID objects within an IoT environment can allow context-aware digital objects to represent physical objects with the abilities to sense, communicate, and interact autonomously [2,10] Powerful adversaries might exist who can monitor all communications, trace tags within a limited time period, corrupt tags, and get side channel information on the reader output. Privacy risks of RFID technology relate to user tracking and localizing, which permit the creation and misuse of detailed user profiles. Thus, it's important that RFID systems provide anonymity, even when the state of a tag has been disclosed.

Wireless sensor networks (WSNs) are another key underlying technology of the IoT network architecture. Given their self-organizing characteristics (to contend with the uncontrollability of the environment), constraints (such as sensor resources and net- work topology constraints), and the wireless transmission medium, WSNs have inherent challenges in protecting privacy and prevent existing techniques (such as public-key ciphers) from being directly transplanted in resource-constrained devices [8]. Privacy in WSNs can be addressed through data orientation (that is, querying data and aggregating sensed data without violating privacy) and context orientation (that is, protecting location and temporal privacy). [9]

Cloud computing provides a virtual infrastructure for IoT to integrate monitoring devices, storage devices, data analytics tools, visualization platforms, and client delivery [12]. This virtual infrastructure would let ubiquitous sensing devices, smart objects, users, and CSPs join the network and collaborate on a single virtual platform. With cloud computing, both individual and cooperating users can access cloud services at a low cost and without possessing expert knowledge of the underlying technologies. Nevertheless, privacy violations can occur, as users might lack control over the data processing. Therefore, the platform CSPs and developers must take responsibility for application privacy. They must protect identity information, the policy components (during negotiation), and transaction histories of the consumers, as well as provide a high degree of transparency in their operations. User lock-in scenarios can also occur when consumers are too dependent on and trusting of a particular IoT CSP. This can be intimidating, particularly when consumers want to migrate from one IoT CSP to another, but they've already revealed important information to the existing CSP and lack control over their data.

VANETS (Vehicular Ad Hoc Networks) embed an on-board unit (OBU) into the vehicle system as a sensing layer node in the IoT [11]. This node communicates to the roadside infrastructure and other peer vehicles. Therefore, establishing secure communication links and providing authentication are two key requirements to enable security and privacy in VANETS. Consequently, the OBU requires additional modules to support information security to ensure user privacy at the same level as identity and location privacy.

Establishing Legal Regulations for IoT Privacy [18-20]

Privacy is a compliance issue sitting at the intersection of social norms, human rights, and legal mandates. In general, the participating countries' legislation is required to support basic privacy principles such as lawfulness and fairness, proportionality, purpose specification, data quality, openness, and accountability. This can be achieved through a collaboration of governmental and private organizations. The European Commission, United Nations' authorities, and other worldwide law enforcement organizations are trying to find a common ground for addressing IoT privacy issues while also empowering the existing legal framework. A strong legal framework should ensure consumers' awareness and their control over the IoT products and services they utilize [10] National-level regulations are not acceptable for IoT privacy because of its global nature. An adequate legal framework should be cross-border and compliant with international legislation, and supplemented by the privacy sector. Although self-regulation is a simpler and less costly solution than state laws for preserving privacy, it's not enough for IoT applications due to their large- scale heterogeneous network deployments. The most challenging issues in establishing legal regulations in IoT privacy are the globally marketed and distributed nature, the durability, the involvement of pervasive environments, and the complexity of the technological developments. [10]

3.2.2 Privacy Findings Based on Existing Solutions

As Section 3.2.1 indicated due to the different facets of the IoT privacy and security is a bug concern from different perspectives. Thus, it needs to be investigated intensively to have a successful solution published and accepted on the markets. How devices are linked to the solution can be individually specified, as long as in the back-end the data can be stored or handle in the correct way to provide it to other services, but for sure this process must respect privacy and security issues in the four mentioned areas shown in Figure 9. [18-20]

After examining the complementary pieces of technology- or application-specific (privacy) frameworks and the IoT network attributes (that is, the technological aspects and legal regulations), the following most important characteristics of an IoT privacy framework were identified (see Figure 10) [2, 18-20]:

- ***Openness, transparency, and a specified purpose****:* Consumers should be aware of the information collected during service time, the purpose of collecting that information, other parties, who will have access to the information, and how that information will be stored.
- ***Identity privacy***: it should not be possible to profile or track consumers based on their user identities.

- ***Temporal and location privacy***: it should not be possible to track or profile consumers based on events or geolocation.
- ***Query privacy***: it should not be possible to pro- file or identify consumers based on the queries they make to service providers.
- ***Access control***: users should have fine-grained access control over the data they give to service providers and be able to tune the granularity of data access depending on the users and queries.
- ***Interoperability***: enable cross-border support of privacy policies among different technologies, standards, and legislation.
- ***Data minimization****:* collect data in lawful and fair ways and limit personal data collection to data needed to perform a given service.
- ***Accountability****:* the consumer and service provider should agree about the controllability and visibility of the service provider's responsibility with respect to the given service or information.
- ***Security****:* safeguard sensitive information against loss, unauthorized access, modification, or disclosure.

The relevance of these principles might vary depending on the contexts of the IoT application scenarios and user requirements. For instance, healthcare, smart home, and surveillance applications have high sensitivity regarding privacy-related frameworks and legal regulations. In addition to these technical characteristics, IoT privacy frameworks should always meet global legal and human rights requirements. [18-20]

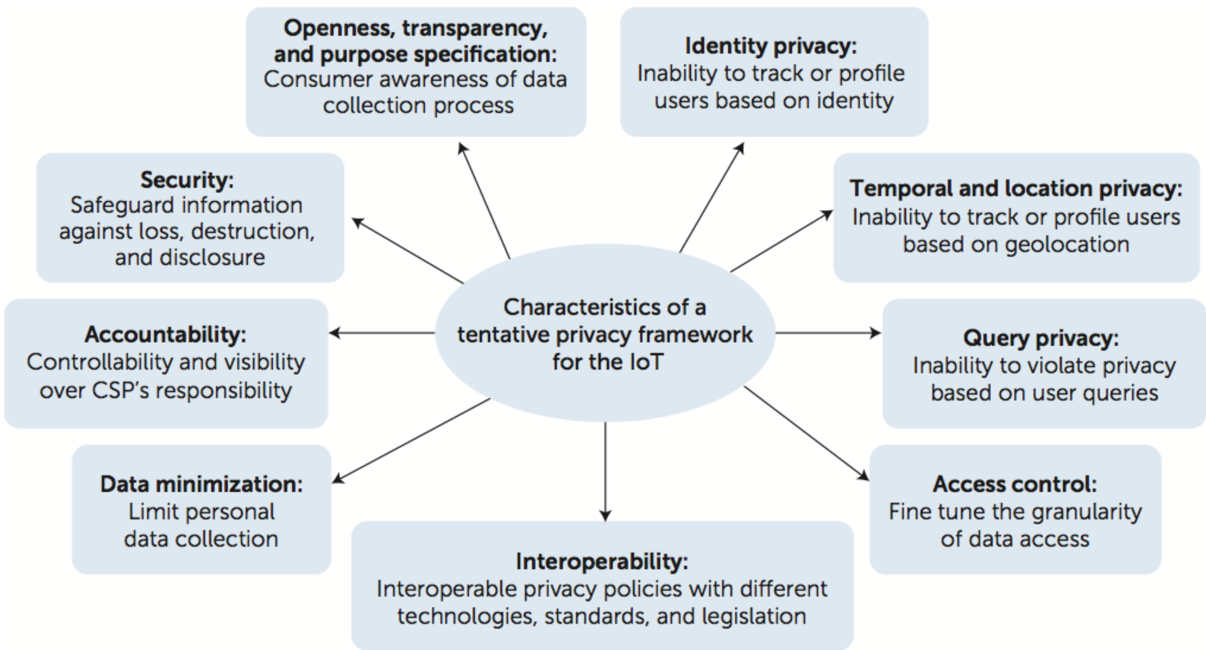

Figure 10: IoT Privacy Framework Characteristics [18-20]

Several privacy-enhancing technologies (PETs) have been proposed for IoT-related applications [10]. Most existing solutions are specific to the underlying technologies or application scenarios. Privacy-oriented cryptographic solutions have been introduced for both internal and external privacy attacks occurring in IoT [13]. However, computationally powerful attackers, who can break cryptographic puzzles might pose threats to these systems. Also, resource-consuming cryptographic operations can create overhead on normal IoT operations. Current PETs for RFID technologies include limiting the distance between the reader and tags, minimalist cryptography, tag renaming and deactivation, access control, and re-encryption. Minimalist cryptography is proposed to perform cryptographic computations at the reader end, storing the resulting information in the tags. The reader can re-encrypt the tag with a different key and write it into its memory in such a way that an eavesdropper gets different encrypted tag signals at different times. Another approach is to use moderate to high-performing devices - that is, proxies - with RFID tags to protect consumer privacy. [18-20]

PETs in RFID have two main objectives: to prevent unauthorized access to RFID tags by establishing secure tag-reader communication, and to pre- serve consumer privacy. The “privacy coach” is an interesting idea for supporting customer privacy in the IoT [12]. A privacy coach is a mobile phone application that supports customers in making privacy decisions when confronted with RFID tags embedded in smart objects. Another approach is to use a proxy as a privacy broker for preserving privacy between service providers and users [12]. This guarantees that both parties obtain required information about the other party; however, privacy proxies can create scalability and interoperability issues in IoT networks. [18-20]

The Unified Modeling Language can be used to document the software requirements of IoT privacy policies, which require high-level abstraction and are suitable for heterogeneous IoT devices and services [2]. Alternatively, user privacy in the IoT can be accomplished by adapting the methodologies available for identity requirements as organizational goals in and location-privacy protection of hosts by exploiting public-key cryptographic algorithms and forwarding agents. Privacy-preservation technologies for data mining include statistical methods for disclosure control, such as k-anonymity, swapping, randomization, micro-aggregation, and synthetic data generation. These methods provide privacy-preserving approaches to the IoT through a data-centric perspective [9]. Cloud computing also adapts different privacy-preserving approaches, including data-centric, accountability, cryptography, access control, authentication, and identity management [12]. More importantly in cloud computing, service-level agreements should be clearly negotiated among stakeholders so they preserve every party’s privacy. However, the technology-specific privacy-protecting mechanisms don’t always provide absolute solutions for the globalized view of IoT privacy preservation. [18-20]

3.3 Business Models on the IoT Market

Looking on the existing solutions on the IoT market including FP7, H2020, and other solutions[5] it can be stated that the chosen business model depends on the funding scheme as well as on the application area. The following three business models were identified:

- Open source
- License fee, meaning “what you pay, you get”
- Closed environment, meaning “buy the product and you get the support”

[5] http://www.smarteremc2.eu/colab/display/SYM/State+of+the+Art (last visit May 9, 2018)

All three models have in common to use social networks (e.g., Facebook and Twitter) and individual homepages to advertise their services.

3.3.1 Open Source Business Model

The first solution with "**open source"** is mainly propagated by the projects and developed solutions from consortiums in FP7 and H2020. There the goal is to be open source to allow many people or services to join the solution. Offering on the one hand the expertise of the consortium and on the other hand to receive feedback by the users, especially in order to extend the provided service or solution. Usually this open source solution is combined with a registration process, in order to have control of solution access and experienced/qualified development. This business model is supported by the following solutions, platforms, and projects described briefly.

AllSeen Alliance (AllJoyn)[6]

The AllJoyn interoperability framework overseen by the AllSeen Alliance (ASA) is probably the most widely adopted open source IoT platform around.

Bug Labs dweet and freeboard[7]

Bug Labs started out making modular, Linux-based Bug hardware gizmos[8], but long ago it morphed into a hardware-agnostic IoT platform for the enterprise. Bug Labs offers a "dweet" messaging and alerts platform and a "freeboard" IoT design app. Dweet helps publish and describe data using a HAPI[9] web API and JSON. Freeboard is a drag-and-drop tool for designing IoT dashboards and visualizations.

DeviceHive[10]

DataArt's AllJoyn-based device management platform runs on cloud services such as Azure, AWS, Apache Mesos, and OpenStack. DeviceHive focuses on Big Data analytics using tools like ElasticSearch, Apache Spark, Cassandra, and Kafka. There's also a gateway component that runs on any device that runs Ubuntu Snappy Core. The modular gateway software interacts with DeviceHive cloud software and IoT protocols, and is deployed as a Snappy Core service.

DSA[11]

Distributed Services Architecture facilitates decentralized device inter-communication, logic, and applications. The DSA project is building a library of Distributed Service Links (DSLinks), which allow protocol translation and data integration with third party sources. DSA offers a scalable network topology consisting of multiple DSLinks running on IoT edge devices connected to a tiered hierarchy of brokers.

Eclipse IoT (Kura)[12]

---

[6] https://allseenalliance.org/ (last visit May 9, 2018)
[7] http://buglabs.net/ (last visit May 9, 2018)
[8] http://linuxdevices.linuxgizmos.com/modular-embedded-computer-adds-cortex-a8-soc-android-support/ (last visit May 9, 2018)
[9] https://hapijs.com/ (last visit May 9, 2018)
[10] http://devicehive.com/ (last visit May 9, 2018)
[11] http://www.iot-dsa.org/ (last visit May 9, 2018)
[12] http://iot.eclipse.org/ (last visit April 9, 2018)

The Eclipse Foundation's IoT efforts are built around its Java/OSGi-based Kura API container and aggregation platform for M2M applications running on service gateways. Kura, which is based on Eurotech's Everywhere Cloud IoT framework[13], is often integrated with Apache-Camel[14], a Java-based rules-based routing and mediation engine. Eclipse IoT sub-projects include the Paho messaging protocol framework, the Mosquitto MQTT stack for lightweight servers, and the Eclipse SmartHome framework. There's also a Java-based implementation of Constrained Application Protocol (CoAP) called Californium, among others.

Kaa[15]

The CyberVision-backed Kaa project offers a scalable, end-to-end IoT framework designed for large cloud-connected IoT networks. The platform includes a REST-enabled server function for services, analytics, and data management, typically deployed as a cluster of nodes coordinated by Apache Zookeeper. Kaa's endpoint SDKs, which support Java, C++ and C development, handle client-server communications, authentication, encryption, persistence, and data marshalling. The SDKs contain server-specific, GUI-enabled schemas translated into IoT object bindings. The schemas govern semantics and abstract the functions of a diverse group of devices.

Macchina.io[16]

Macchina.io provides a "web-enabled, modular and extensible" JavaScript and C++ runtime environment for developing IoT gateway applications running on Linux hacker boards. Macchina.io supports a wide variety of sensors and connection technologies including Tinkerforge bricklets, XBee ZB sensors, GPS/GNSS receivers, serial and GPIO connected devices, and accelerometers.

GE Predix[17]

GE's PaaS (Platform as a Service) software for industrial IoT is based on Cloud Foundry. It adds asset management, device security, and real-time, predictive analytics, and supports heterogeneous data acquisition, storage, and access. GE Predix, which GE developed for its own operations, has become one of the most successful of the enterprise IoT platforms, with about $6 billion in revenues. GE recently partnered with HPE, which will integrate Predix within its own services.

Home Assistant[18]

This up and coming grassroots project offers a Python-oriented approach to home automation. For details see the published profile-on-Home-Assistant[19].

Mainspring[20]

M2MLabs' Java-based framework is aimed at M2M communication in applications such as remote monitoring, fleet management, and smart grids. Like many IoT frameworks,

---

[13] https://www.eurotech.com/en/press+room/news/?672 (last visit May 9, 2018)
[14] http://camel.apache.org/kura.html (last visit May 9, 2018)
[15] http://www.kaaproject.org/ (last visit May 9, 2018)
[16] http://macchina.io/ (last visit May 9, 2018)
[17] https://www.ge.com/digital/predix (last visit May 9, 2018)
[18] https://home-assistant.io/ (last visit May 9, 2018)
[19] https://www.linux.com/news/home-assistant-python-approach-home-automation-video (last visit May 9, 2018)
[20] http://www.m2mlabs.com/framework (last visit May 9, 2018)

Mainspring relies heavily on a REST web-service, and offers device configuration and modeling tools.

Node-RED[21]

This visual wiring tool for Node.js developers features a browser-based flow editor for designing flows among IoT nodes. The nodes can then be quickly deployed as runtimes, and stored and shared using JSON. Endpoints can run on Linux hacker boards, and cloud support includes Docker, IBM Bluemix, AWS, and Azure.

Open Connectivity Foundation (IoTivity)[22]

This amalgamation of the Intel and Samsung backed Open Interconnect Consortium (OIC) organization and the UPnP Forum is working hard to become the leading open source standards group for IoT. The OCF's open source IoTivity project depends on RESTful, JSON, and CoAP.

openHAB[23]

This open source smart home framework can run on any device capable of running a JVM (Java Virtual Machine). The modular stack abstracts all IoT technologies and components into "items," and offers rules, scripts, and support for persistence -- the ability to store device states over time. OpenHAB offers a variety of web-based UIs, and is supported by major Linux hacker boards.

OpenIoT[24]

The mostly Java-based OpenIoT middleware aims to facilitate open, large-scale IoT applications using a utility cloud computing delivery model. The platform includes sensor and sensor network middleware, as well as ontologies, semantic models, and annotations for representing IoT objects.

OpenRemote[25]

Designed for home and building automation, OpenRemote is notable for its wide-ranging support for smart devices and networking specs such as 1-Wire, EnOcean, xPL, Insteon, and X10. Rules, scripts, and events are all supported, and there are cloud-based design tools for UI, installation, and configuration, and remote updates and diagnostics.

OpenThread[26]

Nest's recent open source spin-off[27] of the 6LoWPAN-based Thread wireless networking standard for IoT is also backed by ARM, Microchip's Atmel, Dialog, Qualcomm, and TI. OpenThread implements all Thread networking layers and implements Thread's End Device, Router, Leader, and Border Router roles.

[21] http://nodered.org/ (last visit May 9, 2018)
[22] https://openconnectivity.org/ (last visit May 9, 2018)
[23] http://www.openhab.org/ (last visit May 9, 2018)
[24] https://github.com/OpenIotOrg/openiot (last visit May 9, 2018)
[25] http://www.openremote.org/display/HOME/OpenRemote (last visit May 9, 2018)
[26] https://github.com/openthread/openthread (last visit May 9, 2018)
[27] https://nest.com/press/nest-announces-open-source-implementation-of-thread/ (last visit May 9, 2018)

Physical Web/Eddystone[28]

Google's Physical Web enables Bluetooth Low Energy (BLE) beacons to transmit URLs to your smartphone. It's optimized for Google's Eddystone BLE beacon, which provides an open alternative to Apple's iBeacon. The idea is that pedestrians can interact with any supporting BLE-enabled device such as parking meters, signage, or retail products.

PlatformIO[29]

The Python-based PlatformIO comprises an IDE, a project generator, and a web-based library manager, and is designed for accessing data from microcontroller-based Arduino and ARM Mbed-based endpoints. It offers preconfigured settings for more than 200 boards and integrates with Eclipse, Qt Creator, and other IDEs.

The Thing System[30]

This Node.js based smart home "steward" software claims to support true automation rather than simple notifications. Its self-learning AI software can handle many collaborative Machine-to-Machine actions without requiring human intervention. The lack of a cloud component provides greater security, privacy, and control.

ThingSpeak[31]

The five-year-old ThingSpeak project focuses on sensor logging, location tracking, triggers and alerts, and analysis. ThingSpeak users can tap a version of MATLAB for IoT analysis and visualizations without buying a license from Mathworks.

Zetta[32]

Zetta is a server-oriented, IoT platform built around Node.js, REST, WebSockets, and a flow-based "reactive programming" development philosophy linked with Siren hypermedia APIs. Devices are abstracted as REST APIs and connected with cloud services that include visualization tools and support for machine analytics tools like Splunk[33]. The platform connects end points such as Linux and Arduino hacker boards with cloud platforms such as Heroku in order to create geo-distributed networks.

3.3.2 License Fee Business Model

Option two "license fee" is mainly used by consortia having an overhead in industry, because those consortia had the goal to bring a product on the market to make money. But it has clearly to be stated, that the license fee ranges from some 10 Euros to several hundreds and can be monthly or annual fees. Some projects even give the opportunity to offer different categories that influence the fee rate. So this strategy matches perfectly the motto "what you pay, you get". Depending on what you pay you are able to request and use services (e.g., data storage, hosting, upload and download volumes). Usually, when you have high volume the fee rises. This business model offers access to everyone, who is willing to pay and to use the service.

[28] https://google.github.io/physical-web/ (last visit May 9, 2018)
[29] http://platformio.org/ (last visit May 9, 2018)
[30] http://thethingsystem.com/ (last visit May 9, 2018)
[31] https://thingspeak.com/ (last visit May 9, 2018)
[32] http://www.zettajs.org/ (last visit May 9, 2018)
[33] https://www.splunk.com/ (last visit May 9, 2018)

As a deeper analysis of the aforementioned platforms showed, some state that they offer free software, but usually only a free trial version is available. When going into deeper development areas and using all services, you have to pay fees. A very detailed view on this fact is given in [21]. Very detailed information is available for the IoT platform Carriots as shown in Figure 12 and Amazon Web Services[34] as shown in Figure 11. It requires less payment but depending on the payment the offered services vary a lot.

Further, it can be stated that the range of the license fee depends besides offered services also on the needed hardware. Some projects do not name it license fee, instead they require to buy their hardware and with buying it, the license was in parallel bought to use the software and their services. Examples for this case are the Things Network and wacviot[35].

Monthly Message Volume	US East (N.Virginia)	US East (Ohio)	US West (Oregon)	EU (Ireland)	EU (Frankfurt)	EU (London)	APAC (Mumbai)	APAC (Sydney)	APAC (Seoul)	APAC (Tokyo)	APAC (Singapore)
Up to 1 billion messages	$1.00	$1.00	$1.00	$1.00	$1.20	$1.20	$1.05	$1.65	$1.20	$1.50	$1.65
Next 4 billion messages	$0.80	$0.80	$0.80	$0.80	$0.96	$0.96	$0.84	$1.32	$0.96	$1.20	$1.32
Over 5 billion messages	$0.70	$0.70	$0.70	$0.70	$0.84	$0.84	$0.74	$1.16	$0.84	$1.05	$1.16

Figure 11: Pricing AWS IoT from Amazon per million messages

3.3.3 Closed Environment Business Model

In comparison to the second business model option the third one is intended to serve for a close environment. This means only persons or groups are allowed to access the product and service that are really working in that environment and can prove it (e.g., publications, recommendations). Usually those participants have to pay a high fee as well, but can on the other side request therefor also more specialized solutions and extras (e.g., regulation in data storage, data transfer).

Another possibility of closed environment can be seen from the technology perspective; meaning offered service can only be used if specific technology is used. Here differentiations in the following way are possible:

- Used communication standards
- Special API support, e.g. RESTful API
- Special hardware (e.g., environmental sensors)
- Looking on used communication standards most platforms and projects support any kind of standards ranging from classic wired and wireless connections. For the latter standards like LoRa, IEEE 802.15.4, Bluetooth, and WiFi are used depending on the used devices.
- For each platform or project specific APIs are defined, mostly following the RESTful API concept. Those are used especially for Web services and are one way of providing interoperability between computer systems on the Internet. REST-compliant Web services allow requesting systems to access and manipulate textual

[34] https://aws.amazon.com/iot-core/pricing/?nc1=h_ls (last visit May 31, 2018)
[35] http://dgmatics.com/ (last visit May 9, 2018)

representations of Web resources using a uniform and predefined set of stateless operations. Examples for such Web services are often found in the area of Cloud computing that is nowadays a standard service in IoT. Platforms using such RESTful APIs are Xively[36], Amazon[37], Alpha7[38], Bluemix[39], CoCaine (PaaS)[40], GE Predix[41], HP Helion[42], Mendix[43], and RightScale[44].

FREE	CORPORATE	LITE	PRIVATE CLOUD ON PREMISE
Free (NO CREDIT CARD REQUIRED)	2 €* PER MONTH PER DEVICE	0,50 €* PER MONTH PER DEVICE	Contact us
FOR TESTING AND PROTOTYPING	DEVICES SENDING UP TO 1 MB PER DAY AND MAKING LOTS OF CONNECTIONS	LOTS OF DEVICES SENDING LOW AMOUNT OF DATA. E.G. SMART METER, REMOTE MAINTENANCE	FOR UNLIMITED CONNECTIONS AND DATA STORAGE OR PRIVATE USAGE OR CUSTOM NEEDS
Min. number of devices **1**	Max. number of devices **10**	Max. number of devices **100**	Max. Devices Number **Contact Us**
Max. number of devices **2**	Max. number of devices **Unlimited**	Max. number of devices **Unlimited**	Max. Devices Number **Unlimited****
API KEYS **2**	API KEYS **100**	API KEYS **10**	API KEYS **Unlimited****
Max. accepted streams **500 streams per day** **10 streams per minute**	Max. accepted streams **1500 x device # per day** **50 x device # per minute** e.g. 15000 max. accepted streams per day for 10 devices	Max. accepted streams **25 x device # per day** **5 x device # per minute** e.g. 2500 max. accepted streams per day for 100 devices	Max. accepted streams **Unlimited****
Max. stream size **5 KB**	Max. stream size **10 KB**	Max. stream size **5 KB**	Max. stream size **Unlimited****
Max. stream data storage **5000 KB per day**	Max. stream data storage **1 MB x device # per day** e.g. 10 MB max. stream data storage per day for 10 devices	Max. stream data storage **100 KB x device # per day** e.g. 10 MB max. stream data storage per day for 100 devices	Max. stream data storage **Unlimited****
Data retention **3 months**	Data retention **1 year**	Data retention **1 year**	Data retention **Unlimited****
Max. API requests **1000 per day** **100 per minute**	Max. API requests **1000 x device # per day** **100 x device # per minute** e.g. 10000 max. API requests per day for 10 devices	Max. API requests **100 x device # per day** **10 x device # per minute** e.g. 10000 max. API requests per day for 100 devices	Max. API requests **Unlimited****
SMS API **5 SMS per day** **1 SMS per minute**	SMS API **Free 5 SMS per day** **>6 SMS 0.1€* per unit.**	SMS API **Free 5 SMS per day** **>6 SMS 0.1€* per unit.**	SMS API **Contact Us**
Email API **100 Email per day** **10 Email per minute**	Email API **Free 100 Email per day** **>100 0.50€* per thousand**	Email API **Free 100 Email per day** **>100 0.50€* per thousand**	Email API **Contact Us**
SDK Http Request (Outbound) **1000 Req. per day**	SDK Http Request (Outbound) **1000 Req. x device # per day** e.g. 10000 requests per day for 10 devices	SDK Http Request (Outbound) **25 Req. x device # per day** e.g. 2500 requests per day for 100 devices	SDK Http Request (Outbound) **Unlimited****
Basic Support: Email support (best effort) Developer forum	**Corporate Support:** Phone Support - Contact Us Email support 24 hours response time	**Lite Support:** Phone Support - Contact Us Email support 24 hours response time	**Premium Support:** Different plans available Contact Us
Service Level Agreement **NO**	Service Level Agreement **Different plans available**	Service Level Agreement **Different plans available**	Service Level Agreement **Different plans available**

Limits described her apply to an account
* Taxes not included if applicable - ** Depending on the cloud infrastructure

Figure 12: Pricing Scheme Carriots[45]

[36] https://www.xively.com/ (last visit May 10, 2018)
[37] https://en.wikipedia.org/wiki/Amazon_Web_Services (last visit May 10, 2018)
[38] http://www.alpha7.co/ (last visit May 10, 2018)
[39] https://console.ng.bluemix.net/#/store (last visit May 10, 2018)
[40] https://tech.yandex.com/cocaine/ (last visit May 10, 2018)
[41] https://www.ge.com/digital/predix (last visit May 10, 2018)
[42] https://www.hpe.com/ch/de/solutions/cloud.html (last visit May 10, 2018)
[43] https://www.mendix.com/application-platform-as-a-service/ (last visit May 10, 2018)
[44] https://www.rightscale.com/ (last visit May 10, 2018)
[45] https://www.carriots.com/ (last visit May 8, 2018)

Looking on the area of IoT it is also possible to find services offered for closed environment that require specific hardware. So limiting the user range, due to the request to buy special hardware to use offered services. Perfect examples are the classic security systems that allow using their services only, if you really need security for your living environment.

4 symbIoTe's Status Analysis

This section analyses the relationship and influences between symbIoTe and affected stakeholders by different methodologies. These methodologies are described in Section 4.1 and subsequently applied to each use-case individually. Therefore, Sections 4.2 to 4.6 each focus on one of the five use-cases and apply the different methodologies. It has to be kept in mind that the applied methodology CANVAS (cf. Section 4.1.1) addresses more the Business-to-Customer (B2C) relationship than the Business-to-Business (B2B) relationship and, thus, it is essential combine CANVAS with another method (here: Value-Network-Analysis see Section 4.1.3) to cover this. As a third pillar towards the envisioned business model recommendation tussles need to be identified (cf. Section 4.1.2), because the technology or solutions brought to the market may influence existing technologies, solutions, or even stakeholder behavior. The main inputs for all three methods are the list of stakeholders involved and the applied use-case itself. Due to the fact that all three methods include different aspects from the business perspective the list of stakeholders involved is slightly changing throughout the methods. Hence, each section will have a variance in place here.

4.1 Methodologies Applied

This section describes the three methodologies that are applied to all five use-cases in order to analyze symbIoTe's relationship with different stakeholders addressing B2C and B2B relationship. All those are use-case specific, because without a use-case in place a valid business model recommendation becomes impossible. The selected order of the three methods is CANVAS, Tussle Analysis, and Value-Network-Analysis, because they build on each other in terms of structure and information received.

4.1.1 symbIoTe's CANVAS Use-case Owner View

In Deliverable D1.3 [15] for each use-case a CANVAS was filled out following the leading questions from Osterwald et al. [14, 16]. The business model CANVAS includes the most widely used components in the business model literature, namely customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, and cost structure [7]. Each of these components tries to answer specific questions to build a business model for a special purpose (e.g., company, project) [16,17]:

- **Key partners**:
    - Who are our key partners? Who are our key suppliers? Which key resources are we acquiring from partner? Which key activities do partners perform?
- **Key activities**:
    - What key activities do our value propositions, our distribution channels, customer relationships, and revenue streams require?
- **Value propositions**:
    - What value do we deliver to the customer? Which one of our customer's problems are we helping to solve? What bundles of products and services are we offering to each customer segment? Which customer needs are we satisfying?

- **Customer relationships**:
  - What type of relationship does each of our customer segments expect us to establish and maintain with them? Which ones have we established? How are they integrated with the rest of our business model? How costly are they?
- **Customer segments**:
  - For whom are we creating value? Who are our most important customers?
- **Key resources**:
  - What key resources do our value propositions, our distribution channels, customer relationships, and revenue streams require?
- **Channels**:
  - Through which channels do our customer segments want to be reached? How are we reaching them now? How are our channels integrated? Which ones work best? Which ones are most cost-efficient? How are we integrating them with customer routines?
- **Cost structure**:
  - What are the most important costs inherent in our business model? Which key resources are most expensive? Which key activities are most expensive?
- **Revenue streams**:
  - For what value are our customers really willing to pay? For what do they currently pay? How are they currently paying? How would they prefer to pay? How much does each revenue stream contribute to overall revenues?

Combining all five initial CANVASes to one together the resulting CANVAS as illustrated in Figure 13 was received. Purple are issues related to citizens, green are issues related to developers, and red indicate general issues. Some of the mentioned items are highlighted in bold and underlined indicating that a minimum of two use-case includes this item in the relevant building block. From this point on the development of solutions within symbIoTe continued having those collected items in mind and each use-case picked out relevant items out to focus on them and/or to specify them in more detail throughout the different work packages in symbIoTe.

Over the project time use-cases became more specified resulting sometimes in show-cases and, thus, it was necessary to repeat the CANVAS fill out due to two main reasons:

1. In order to receive a valid and up-to-date input for the intended business model recommendation for Deliverable D1.5.
2. In order to receive valid and up-to-date input for the two other methods applied to cover the B2B aspect in the VNA and the socio-economic impact of symbIoTe identified by the TA.

Further the updated CANVAS now specifies in more detail which parts of symbIoTe will be used to develop the case, as well as a more focused value proposition. In Figure 13 some items were highlighted in bold, those stayed the same in the second iteration of CANVAS main differences could be identified in key activities, key resources, and value proposition when going into detail for each use-case. Drawing a final overall CANVAS for the second iteration would be to complex and confusing and, thus, another figure showing the summarized CANVAS for second iteration was omitted here.

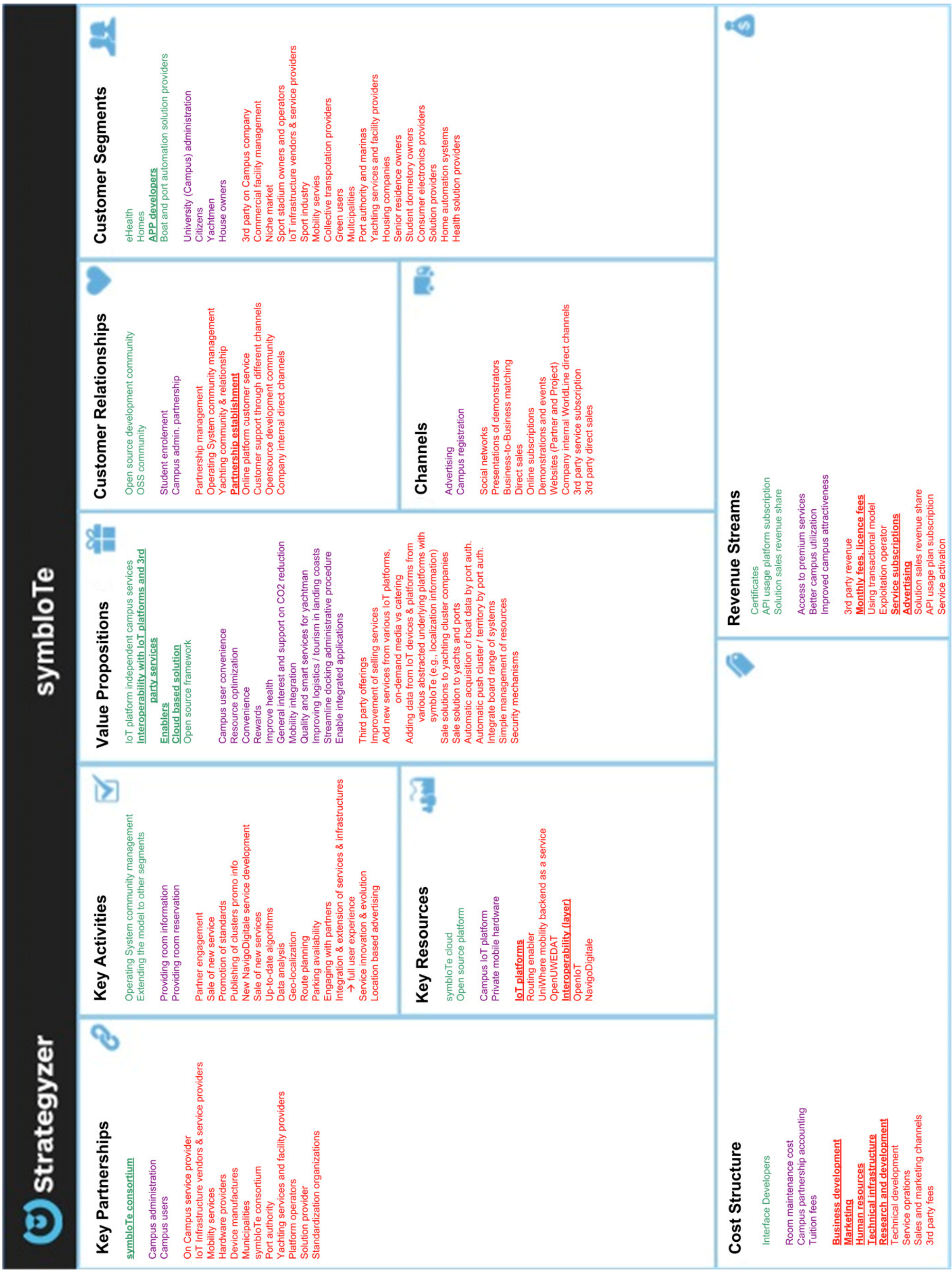

Figure 13: Overall filled out initial CANVAS for total symbIoTe

4.1.2 Tussle Analysis

Clark et al. [25] were the first to point out the relevance of tussles in the future cyberspace. Based on this argumentation, the SESERV FP7-project defined, introduced, and successfully applied the tussle analysis to a variety of different FP7 projects [26]. In a first step, tussle analysis identifies stakeholders and their interests. In a second step, conflicts between these interests and means available to stakeholders to enforce their interests are identified. In the last step, it is investigated, how stakeholders will use their means to enforce their interests and how this can either be prevented or at least ensured that no affected stakeholder suffers from unfair consequences. Such anticipatory evaluation of technology is particularly important, when the technology proposes use-cases that are as novel and innovative as the use cases proposed by symbIoTe. Due to the successful application of tussle analysis by SESERV, tussles analysis was standardized by an ITU recommendation [27] and also applied by the SmartenIT [28] and FLAMINGO project [29].

Tussle analysis will substantiate decisions taken by symbIoTe and point out issues that still have to be addressed by the symbIoTe consortium. The tussle analysis for each use case will first give an overview of the use-case with aspects relevant for the subsequently performed tussle analysis and next identify all relevant stakeholders. It is important to understand that every entity that is somehow affected by the technology is termed stakeholder and not only those, who provide value. Therefore, also criminals are termed stakeholders. After stakeholders are identified and discussed, an adoption tussle is identified for three of the five use case. This adoption tussle identifies interest conflicts with stakeholders that may prevent symbIoTe from making it to market and being widely deployed. Therefore, it is essential that these adoption tussles are solved; as otherwise, symbIoTe may never make it to market. The tussles discussed after the adoption tussle make the assumption that the adoption tussle is solved successfully and the symbIoTe solution is already in production as assumed by the use cases. Each tussle analysis section closes by discussing the implications the tussle analysis has for symbIoTe and according next steps to be taken by the symbIoTe consortium.

4.1.3 Value Network Analysis

Traditional business model approaches, like the business CANVAS [14, 16] try to highlight the processes within the business and show an inside out perspective on the business or in this case symbIoTe. A Value Network Analysis in contrast reflects a more global objective view from the business model ecosystem in general. The goal is to not only obtain the value creation of the business in question, but rather explain the relations between the stakeholders in the whole value creation process. This is especially crucial for the value creation process of an IoT-Platform, which connects stakeholder with each other and enables to build the value creating network, but create minimal value itself. In order to map the network of an ecosystem research suggested to consider stakeholder, actions and value transactions within the network [38, 39]. In contrast to traditional business model theory with value creation and value capture as main purpose, Westermund et al. defined in their *Value Design* approach four aspects which are to consider in the field of IoT, namely (cf. Figure 14): value driver, value nodes, value exchange, and value extract [41].

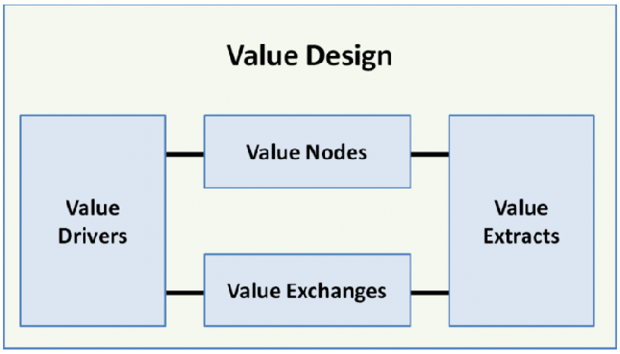

Figure 14: Key pillars of a business model design tool for IoT ecosystems [41].

Value driver: In order to form a value network future participants have to be motivated to take part in the whole process or so called *value drivers*. Motivations form individually or shared with other participants of the network, however a need to create value and make money is critical to create a sustainable value network.

Value nodes: While more traditional approaches of the VNA limits the role of actors to real persons, groups, organizations, business units or similar actors [40], Westermund et al. consider in the context of IoT as well actions, automated processes, autonomous actors, such as programmed systems, learning systems or smart sensors as long as they provide value to the IoT system. In the context of this paper we will address the value nodes as stakeholders for consistency reason.

Value exchange: V. Allen defined the value flows in a value network as tangible and intangible transactions [40]. Thus, different forms of value exchange are part of the system e.g. knowledge, information, money, and resources and describe the relation between the actors. *Value exchanges* not only describes how the system works, furthermore it shows how revenue gets created.

Value extraction: For the commercialization of the product or system the extraction of monetary value is crucial. This dimension focuses on the extraction of value relevant for the own business rather than the whole system. Depending on the ecosystem this can be based on single interactions or multiple.

The *Value design* helps to understands on how the value is created and captured within a IoT network. While this framework is used as a mental model for creating the VNA's based on definitions in deliverable D1.3 [15] and D5.2 [35], there is no use of the terminology introduced by Westermund et al. [40]. Further discussions with the involved partners took place in order to complete the initially designed VNA by the end of March 2018.

The stakeholder list in context of the VNA is considering previously proposed stakeholders by CANVAS and TA, but amended the list to fit the perspective of the VNA. Thus, some stakeholder are excluded, but other stakeholders might are included.

4.2 Use-Case 1: Smart Residence

This section analysis the Smart Residence use-case by presenting a CANVAS analysis in Section 4.2.1, applying tussle analysis in Section 4.2.2, and finally conducting a value network analysis in Section 4.3.3.

4.2.1 CANVAS Use-case Owner View

In Deliverable D1.3 [15] the initial version of the CANVAS for the use-case Smart Residence was presented. The CANVAS building blocks were filled with input available end of 2016. Within the last 1.5 years some changes in the use-case have occurred, so that a new iteration of CANVAS was necessary to illustrate the current state. This status is based on the input provided by use-case owners and contributors, as well as on available more detailed description of use-cases and their intended show-cases as described in Deliverable D5.2 [35].

The involved partners decided as justified in Deliverable D5.2 [35]. that the use-case Smart Residence will cover three show-cases, namely (1) Healthy Indoor Air, (2) Smart Residence with focus on smart area control, and (3) Active and Assisted Living (AAL). Thus, the original CANVAS is now updated by three separate ones but both showing similarities in different building boxes (e.g., cost structure and key partnerships).

The purpose of **show-case (1) - Health Indoor Air** - is to monitor and improve indoor air quality. Indoor air quality (IAQ) refers to the quality of the air inside buildings as represented by concentrations of pollutants and thermal (temperature and relative humidity) conditions that affect the health, comfort and performance of occupants. It is important to ensure that the air inside the building we inhabit on a daily basis is of a good quality. Outdoor generated air pollution is relevant for indoor air quality and health. Exposure to indoor air pollution has been linked to the development of different diseases from infections to asthma or to poor sleep. It can also cause less serious side effects such as headaches, dry eyes and nasal congestion. Sensing and Control Systems SL partner's (S&C) roadmap aims to create a smart home/office connected with the city.

The resulting CANVAS is illustrated in Figure 15 and includes items with general purpose and not further specified to issues related to citizens or developers. As it can be seen in comparison to the initial CANVAS in Deliver D1.3, a more concrete view on involved key partners, value proposition, and cost structure is in place. Further, the involved key resources could be now identified clearly, especially with a matching to the symbIoTe core services (here: IoT Resource Discovery and Access / Domain Enablers (L1) and IoT Platform Federation (L2)) used. This show-case has a general value proposition in mind by establishing healthier indoor spaces and creating new partnerships, which is also reflected by the intended customer relationships, customer segments, and channels used. The planned revenue stream used follows the approach of license fee business models (cf. Section 3.3.2) and having additional agreements in place allowing them to use data collected. As it can be seen in Figure 15 the cost structure is complex and, thus, will highly influence the license fee.

Show-case (2) goes on **Smart Residence** itself and it is designed to show the potential of residential automation applications, where home platforms interoperate in order to provide a comfortable environment to the users. The envisioned scenarios depict two cases: in the first one home devices are constantly driven to keep a comfortable ambience, in the second one an application dynamically changes its interface depending on the user location.

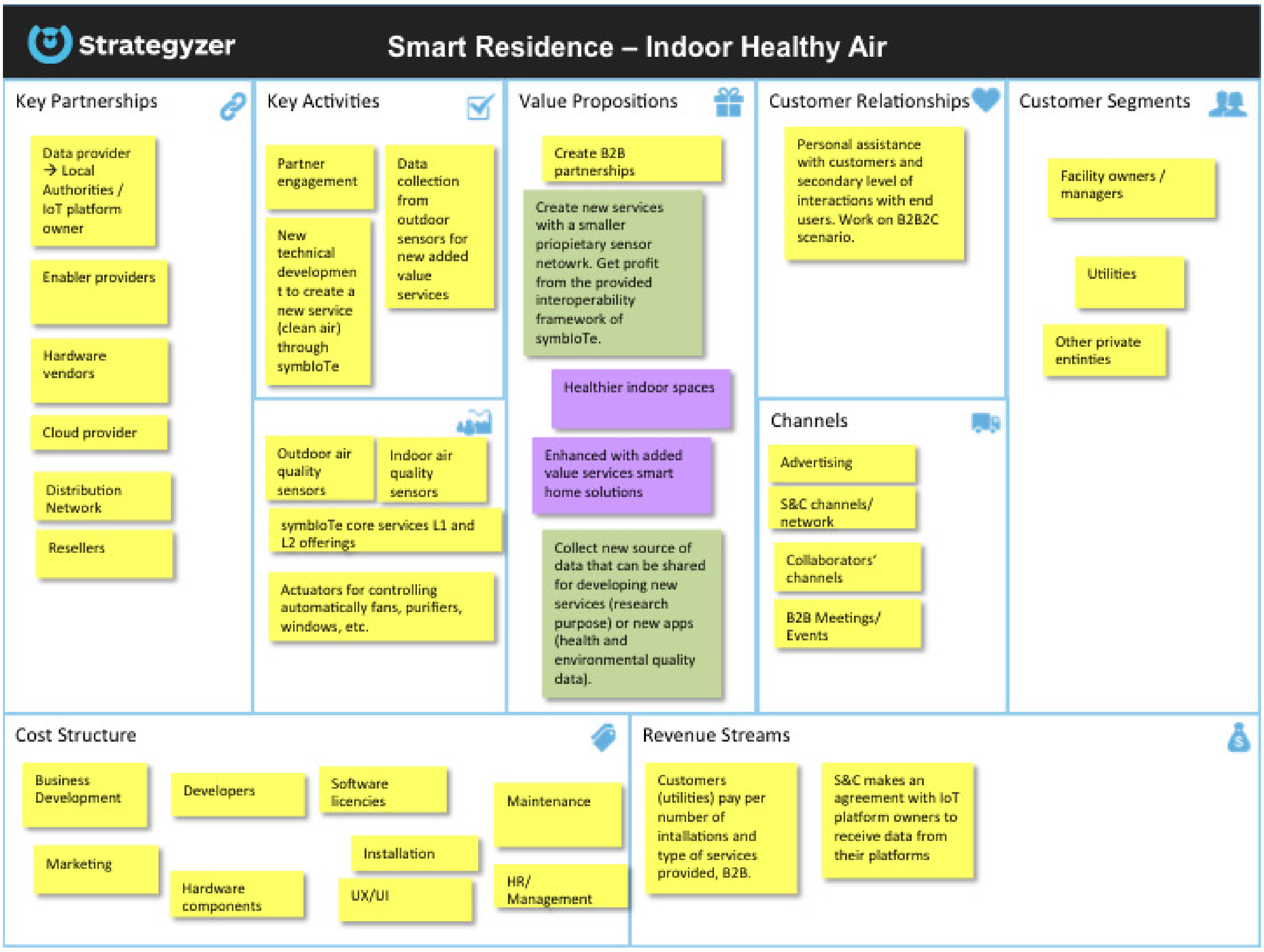

Figure 15: CANVAS for show-case "Healthy Indoor Air"[46]

The resulting CANVAS is shown in Figure 16, where the coloring indicates the following: Purple entries are issues related to citizens, green entries are issues related to developers, and yellow entries indicate general issues. In comparison to Figure 15 this show-case (2) has also standardization organizations and solution providers in mind for key partnerships, but not enabler and data providers. The key activities are similar, but also include promotion of standards due to the additional stakeholder group. In case of key resources the used sensors come more from home automation sector (e.g., lights, dimmers, automated curtains, etc.) and similar to the other show-case interoperability and symbIoTe services are supported. Additionally, open source platforms should be integrated into the solution. Besides advertising and using own channels presentation options like IoT events, social networks, demonstration events, and marketing campaign stands in the focus also. The intended cost structure is as complex as in show-case (1) and, thus, clearly call also for license fee business model eventually combined with subscriptions. An agreement on data usage itself is at the moment not intended, but users have to pay for maintenance, updates, and hardware installation separately, as well if they want to have high security in place by using certificates.

[46] UX/UI = User Experience/ User Interphase (this is for designing the solution)

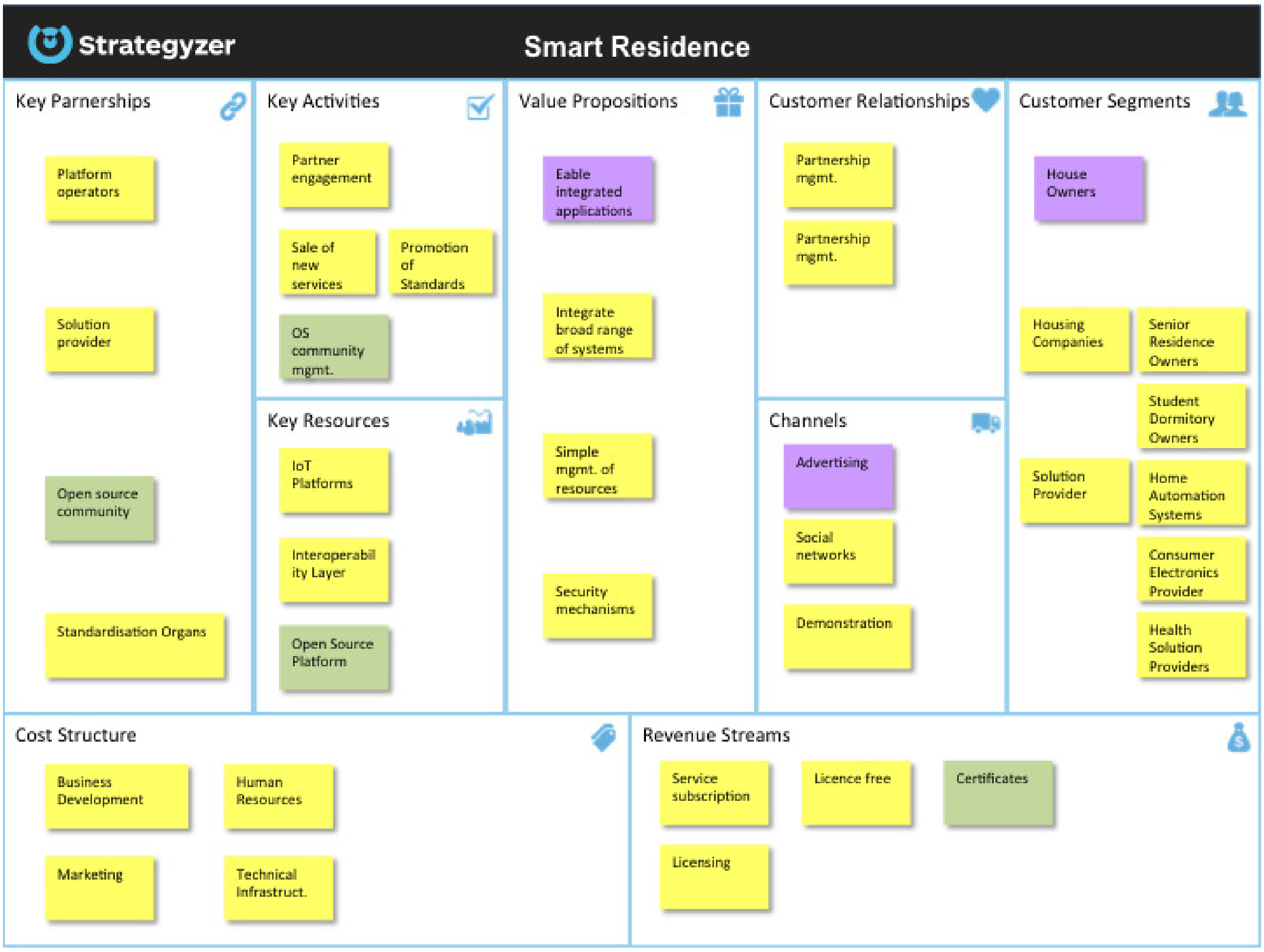

Figure 16: Show-case “Smart Residence”

Show-case (3) addresses the topic of **active and assisted living (AAL)** in future residences. The idea behind this show-case to provide elderly people potentially suffering from chronic diseases such as heart failure or diabetes with pervasive user interfaces (embedded in the smart home) that support them in managing their health through regular measurement of vital parameters. The overall goal is to improve overall life quality, reduce hospitalization rates and to enable elderly people to live an independent life. Within the show-case an interactive, voice-enabled smart mirror detects the presence of residents and fetches a health profile from a remote healthcare center server. This profile might contain a medication schedule or instructions for measuring vital parameters (e.g. blood pressure, blood glucose) on regular intervals. The smart mirror interacts with medical sensors, guides the end-user through the measurement process and finally transmits all data to the health data center for review by a caretakers or health professionals.

The resulting CANVAS is shown in Figure 17 and shows in the building blocks many similarities to show-case (1). This fact was expected, because the general purpose of improving living quality is the same. The only difference is the application scenario. Thus, the key activities are the same, except the item on data collection from outdoor sensors is missing here. The value proposition has also creating partnerships and healthier environment (here: for elderly people) in place and additionally smart and intuitive monitoring on top of smart home solution that is the focus of show-case (2). The envisioned customer relationships have included personal assistance with customers through healthcare professionals additionally. The planned channels to be used are the same as in show-case (1), which also belongs to the expected cost structure. The cost structure includes also the reimbursements for healthcare professionals due to the application service. For the revenue streams the services provided through private/public health insurance program is an add-on for show-case (3). Similar to the other two show-cases the third one has the symbIoTe core services (Platform Integration Level 1 (L1) and Integration Level 2 (L2)) mentioned in the key resources needed for the scenario to run successfully.

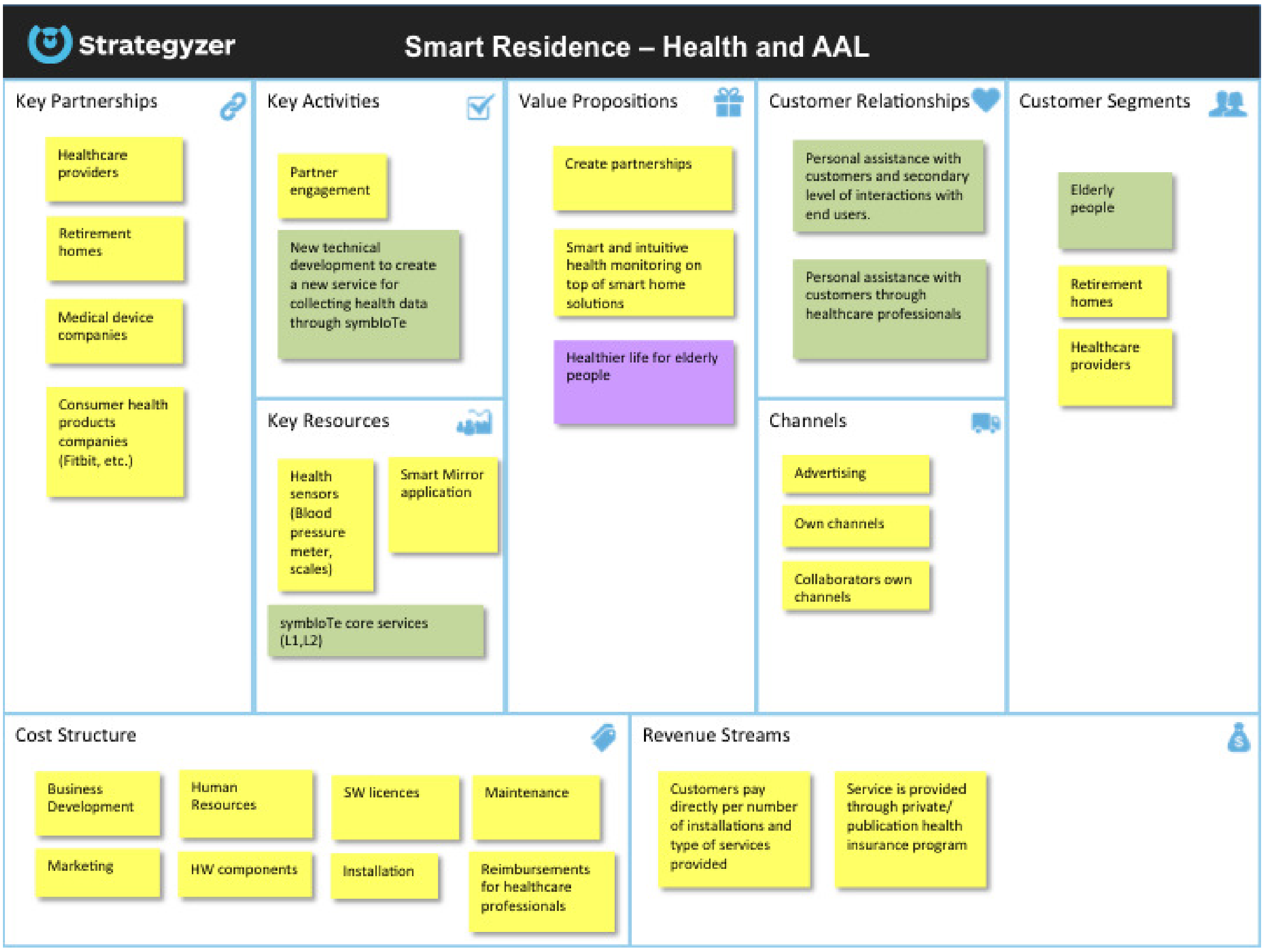

Figure 17: CANVAS for show-case “Active and Assisted Living”

The main differences for the first two show-cases can be found in the following building blocks:

- Building block “value proposition”: Show-case (1) focuses on partnership creation, enhancement of added value services for smart home solutions (e.g., energy usage, security), and healthier indoor spaces in general. In comparison show-case (2) sees its value proposition in enabling integrated applications, integration of broad range of systems (e.g. light systems, motorized curtain systems, etc.), simplifying management of resources, security support, and integration of multiple platforms in the same environment (e.g., flat, office).

- Building block "customer relations": Show-case (1) intends to have personal assistance with customers in place, as well as secondary level interactions as B2B2C-model[47] with end-users. Whereas show-case (2) sees the customer's relationship more in the area of management partnerships in general, assisting and maintaining users, and support by software updates.
- Building block "customer segments": Here show-case (1) clearly focuses on facility owners/managers, utilities, and other private entities. In comparison show-case (2) focus on house owners and housing companies with strong focus on smart living aspects, as well as on entities that are responsible for products integrated in such an environment (e.g., solution providers for home automating systems, consumer electronic providers).

As pointed out before show-case (1) and showcase (3) are quite similar and, thus, here are only listed the main difference between those two and the listings of differences to show-case (2) are neglected:

- The envisioned key partnerships are completely different compared to show-case (1) and, thus, also to show-case (2). Here healthcare providers, retirement homes, medical device companies, and consumer healthier product companies (e.g., Fitbit) are in focus.
- Another difference is in place in the key resources, where show-case (3) addresses items such as health sensors (e.g., blood pressure meter, scales) and smart mirror application equipment that are planned to monitor the elderly people in their environment.
- The last big difference can be found in the customer segment that is obvious due to a change of the application area within the Smart Residence idea. Here elderly people, retirement homes, and healthcare providers need to be mentioned for show-case (3).

4.2.2 Tussle Analysis

The smart residence use case aims to integrate symbIoTe into smart homes. In particular, symbIoTe is designated to provide communication and interoperability between various smart home devices. Section 4.2.2.1 lays the ground for the discussion by identifying all involved stakeholders and their interests. The tussle discussed in Section 4.2.2.2 raises the question of how the adoption of symbIoTe can be ensured. This question arises because big solution providers have the interest of monopolizing the smart home market by establishing their proprietary solutions. The tussle discussed in Section 4.2.2.3 shows that many of the functionalities envisioned by the use case threaten the safety of residents, if exploited by criminal third parties. These functionalities are, for example, the opening of doors and curtains via smartphones and the tracking of, processing of, and reacting to (in terms of medication and workout prompts) residents' vital signs. It is argued that only according security mechanisms can prevent such exploits, confirming symbIoTe's approach of putting security first. Furthermore, it is shown how Distributed Denial of

[47] Assuming a direct client is a utility receiving support by symbIoTe contact. Their clients use the smart home and the utilities give support to them. If the utility fails to help them in a second level symbIoTe contact provides help to end-users.

Service (DDoS) attacks can be prevented by judicial and accompanying technical means. The tussle discussed in Section 4.2.2.4 points out the key role of smart home gateways. Section 4.2.2.5 highlights implications that the tussle analysis has for the next steps to be undertaken by the symbIoTe consortium.

4.2.2.1 Stakeholders and Interests

Deliverable D1.3 [15] distinguishes three main user segments for this use case, namely house owners, housing companies, and solution providers. House owners and housing companies take different parts in physically owning, operating and managing homes. As their interests and functions are similar, they do not need to be distinguished for the subsequent tussle analysis. Thus, they are collectively referred to as house operators. House operators aim at (i) satisfying residents in order to increase their reputation and, therefore, potential future customers and at (ii) minimizing managerial and operational costs in order to maximize their revenue. Residents have not been listed in D1.3 but play a key role as they physically inhabit homes. Therefore, their interests are being able to rely on their smart home to provide safety and security and using it in a convenient manner. Solution providers, as discussed in D1.3, provide different smart home devices and services/software. In order to increase their customer base, they want to be able to provide easy-to-use solutions. Note that interoperability may not be in the interests of all solutions providers, as large solution providers may try to monopolize the market by locking customers into an ecosystem that only operates with their devices. Companies that depend on Internet access and presence, which nowadays virtually includes all companies, are a passive stakeholder in this use case. They are involved, as criminals can threaten and blackmail them with smart home device supported DDoS attacks. Those criminals are the last stakeholder group and can be described as individuals or more likely groups of individuals, who exploit vulnerabilities of the smart home to make money. This can be done by robbing residents or by blackmailing other companies. Table 1 summarizes the stakeholders and their interests.

Additional stakeholders that are involved in the Smart Residence use case but are not involved in any of the tussles identified are (a) technical operators (install and maintain smart home infrastructure), (ii) social service providers (e.g., nurses, doctors), and (iii) residents' dependents (they communicate with and support elderly residents).

Table 1: Stakeholders and their interests for the smart residence use-case.

Stakeholder	Interests
House operators	Satisfy residents, minimize costs
Residents	Rely on smart home safety, use it conveniently
Device vendors	Maximize sells, monopolize the market
Internet based companies	Achieve high uptime uninterrupted by DDoS
Criminals	Blackmail/DDoS companies, rob residents

4.2.2.2 Adoption Tussle

symbIoTe is open source and will allow to integrate devices from various solution providers. This is good for the residents and house operators, as it avoids being locked into a specific solution provider and having to pay a “monopoly fee”. However, as D1.3 [15] states, large solution providers will try "to push their solutions and standards into the market and thus, to exclude others by creating controlled environments." In other words, solution providers try to monopolize the smart home market by locking customers into their ecosystem. Thus, solution providers need incentive to support symbIoTe and, thereby, greatly aid the adoption of symbIoTe and the compatibility of devices of different solution providers. This incentive is hard to provide for solution providers that have already established themselves in the market. In contrast, it will be easier to go for the support of small solution providers and offer them a way make their solutions interoperable. In particular, given the seamless interoperability that symbIoTe aims for, supporting symbIoTe will allow small solution providers to form a monolithic solution provider on a technical level and, therefore, be as attractive to residents and house operators as the already established solution providers, who may have no incentive to support symbIoTe. This support of smaller solution providers has to be attained by according presentations, advertisements, and networking activities of the symbIoTe consortium with solution providers in question.

The adoption of symbIoTe in the smart home environment can further be supported by promoting symbIoTe's ability to avoid login effects of house operators and customers.
In particular, making house operators and residents aware of potential login-effects and symbIoTe's capability to avoid such login effects, will force large solution providers to also support symbIoTe. The reason is that house operators and residents form the customer base of all solution providers and, if this customer base demands symbIoTe-compliant devices, this will force solution providers to support symbIoTe. Thus, residents and house operators have to be aware of the advantages that symbIoTe offers. This awareness has to be fostered by convincing demonstrations of symbIoTe. However, the advantages shown in these demonstrations have to go beyond the simple avoidance of lock-in effects. Additionally, also arguments with respect to expenses of updates, simplicity and usability, and security over lifetime (cf. Section 4.2.2.3) of symbIoTe devices will be important in order to convince house operators and residents.

Note that it is likely more effective to go for the support of house operators than for residents. The reason is that house operators are enterprises and, therefore, (i) can be convinced by long-term, economic, strategic arguments, and (ii) decide over the smart home devices in a large number of homes. In contrast, residents are more prone to make short-term, impulsive, advertisement driven decisions.

4.2.2.3 Security Tussle

The discussion in this section is illustrated in Figure 18. As stated above, it is assumed that the adoption tussle is solved successfully and, therefore, the symbIoTe solution deployed in smart homes. Security of smart home devices is critical for various reasons, as discussed below. Unfortunately, solution providers have incentive to produce insecure devices or write insecure software as also discussed. This results in tussles that will negatively impact end-users of insufficient technical literacy, if no according counter-measures are taken. Therefore, the discussion in this section closes by outlining how incentive can be provided to solution providers to provide secure solutions and, therefore, protect end-users from various safety threads and the Internet from an army of smart home devices that participate in DDoS attacks.

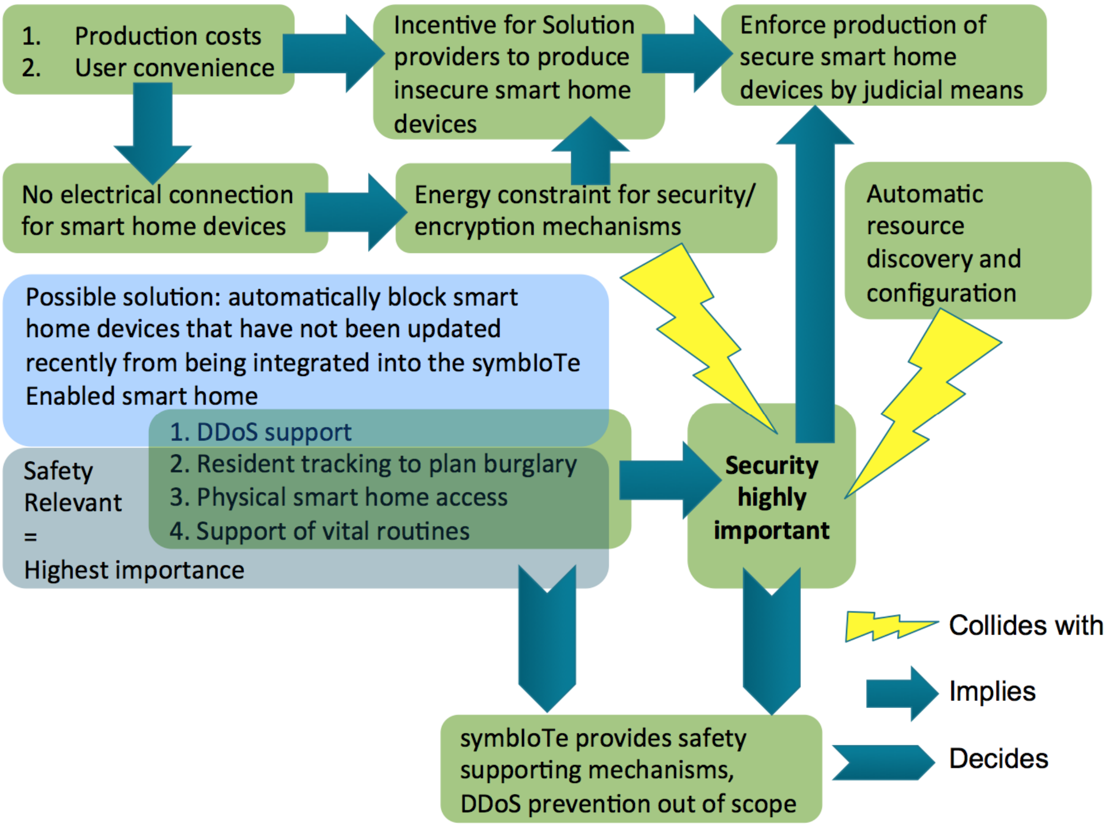

Figure 18: Illustration of the arguments made for the security tussle in Section 4.2.2.3

4.2.2.3.1 DDoS Support

IoT devices (which includes smart home devices) are expected to outnumber other electronic devices, such as smartphones and computers, in the future. This makes them perfectly suited for being recruited for DDoS attacks. Already nowadays reports of IoT-based DDoS attacks increase, which is mainly due to the low security capabilities of many IoT devices. Such DDoS attacks are used to effectively impair the online availability of companies. As such availability is essential, it is the perfect lever to blackmail these companies.

4.2.2.3.2 Resident Tracking to plan burglary

The residents' position in the house is tracked to enable energy savings. If criminals get access to this information over a period of time, they are able to predict when the house will be empty and, thereby, determine the "most convenient" time for a burglary. A related problem is that criminals can monitor the Wi-Fi traffic patterns inside a house to determine, when the house is empty. In this case, it is not even necessary to decrypt the traffic, as the mere packet pattern will already be sufficiently conclusive. Note that this problem not only arises in a smart home context, as it is already possible nowadays to monitor network traffic inside a house, in order to determine whether a house is empty. However, this problem will be magnified in an IoT world, as monitoring devices become more affordable.

4.2.2.3.3 Physical Home Access

Smart home devices enable physical entry to homes. The resident shall be able to open door locks or motorized curtains via smartphones or other electronic devices. Therefore, a hacked device literally “opens the door” for criminals.

4.2.2.3.4 Support of Vital Routines

Smart home devices, as envisioned by symbIoTe, support vital routines by reminding residents to take medication. Therefore, if these reminders are wrong/inaccurate serious health risks arise. This vital role of the correctness of reminders can be monetized via ransom. In particular, cyber criminals can hack the smart home, such that they are able to give wrong prescriptions (alternatively they can corrupt measurements such as insulin levels). Subsequently, they blackmail the solution providers by threatening the resident's health/life by wrong intake reminders.

4.2.2.3.5 symbIoTe Actively Resolves These Tussles

The issues above show the high importance of security capabilities of smart home devices. Notably, all but the first issues imply safety concerns and are, therefore, mandatory to be resolved. Moreover and in line with the saying “Trust takes years to build, seconds to break and forever to repair.” already one safety incident will be sufficient to permanently impair residents’ trust in house operators and solution providers. Therefore, symbIoTe carefully deploys privacy and security supporting authentication and encryption mechanisms and anomaly detection, to address these safety critical issues. Although Section 4.2.2.3.7 argues how a middleware technology like symbIoTe can help to prevent IoT based DDoS attacks, such prevention is considered out of scope for symbIoTe.

4.2.2.3.6 Security Requirements Conflicts Devices Producer Interests

Solution providers are the stakeholder group that manufactures smart home devices. Unfortunately they have an inherent interest to produce insecure devices, as shown next. Many items, such as carpets or door locks, are designated to become smart home enabled but lack an electrical connection. Solution providers will not want to add such a connection, as this increases production costs and decreases the usability/convenience of these devices. This results in harsh energy constraints of the items, which prohibit the use of compute intensive security mechanisms. Also the goal of "automatic resource discovery for dynamic configuration of available services." as stated in D1.3 potentially threatens security. Therefore, solution providers have incentive to maximize sells by flooding the market with insecure devices. Some house operators and residents will be ignorant or oblivious to the fact that deploying such devices threaten residents’ safety (by not being able to support safety relevant security mechanisms) and others (by DDoS attacks).

4.2.2.3.7 Judicial Solution

Since there is no economic incentive for solution providers to produce technically secure smart home devices, a judicial solution suggests itself. In particular, the only solution that was discovered in this analysis, is adopting laws that prohibit the use of devices that are insecure, i.e., declare the use of devices that lack support for a certain set of security algorithms/mechanisms or are not updated regularly illegal. However, such judicial solution has to be supported by according technical means. A middleware like symbIoTe can provide such support by testing when devices last have been updated or even testing them for the security mechanisms they support or exploits they are vulnerable to (the latter two tests are significantly harder to implement than the first). If these tests reveal the device is insecure, e.g. it has not been updated in the last 6 months, it can be blocked from being integrated in the smart home. Therefore, even house operators and residents who are not concerned with the security of their devices (be it because of ignorance or inexperience) will have incentive to only buy sufficiently secure smart home devices. This, in turn, gives incentive to solution providers to produce secure devices. While this judicial enforcement of security is one viable solution, the search for alternatives has to be continued due to the devastating effects insecure devices will have on the future IT landscape. In particular, with the increasing importance of the Internet and the ever-strengthening connection between the digital and physical world, the importance that IoT devices only adhere to their owner and not participate in DDoS or other attacks increases steadily.

The importance to preclude smart homes' vulnerability to DDoS participation becomes evident, when looking at the rapidly increasing number of machines that are part of botnets already [30]. Therefore, legislation has to be deployed as a tool to stop this cyber-epidemic. However, such legislative steps have to be materialized by according technical measures as the majority of users is expected to not possess the technical knowhow to comply with laws that, for example, prohibit the use of devices that not support certain security mechanisms or ensure timely updates.

4.2.2.4 Gateway Tussle

Resident user data is valuable. Any solution provider that manufactures a central entity of a smart home has access to this data. In particular, gateways have a critical function as they are traversed by all data exchanged with the Internet. Therefore, gateway manufacturers can theoretically equip their gateways with firmware that provides them with residents' user data that can be monetized in different ways. However, such eavesdropping of data, although technically possible and hard to detect, is illegal. Therefore, symbIoTe makes the assumption that gateways are trustworthy. In particular, it is necessary to trust some devices in the smart home and extend the trust to others from there. If no device would be trustworthy, it would be possible to construct scenarios, where it is impossible to implement a secure ecosystem. Due to the gateway's vital role, it is best suited to be trusted initially and extend the trust.

4.2.2.5 Implications for symbIoTe

The adoption tussle discussed in Section 4.2.2.2 has shown that the symbIoTe consortium has to convince key stakeholders to ensure symbIoTe's successful introduction to the market despite the resistance faced from monopoly seeking large solution providers. In particular, it was argued that small solution providers have to be convinced of supporting symbIoTe with the main argument that symbIoTe allows them to form a federation that enables competing with big solution providers. Also house operators and residents have to be convinced with the argument that symbIoTe spares them from being locked into the ecosystem of a monopolistic large solution provider. However, also arguments with respect to expenses of updates, simplicity and usability, and security over lifetime (cf. Section 4.2.2.3) of symbIoTe devices will be important to convince house operators and residents. Therefore, the symbIoTe consortium has to pay special attention to these aspects in the current implementation efforts to ensure that they will be strong arguments for deploying symbIoTe.

To convince all stakeholders mentioned above, it is important to prove the seamless integration and interoperability enabled through symbIoTe. If this seamless integration and interoperability cannot be achieved, small solution providers will not be convinced that symbIoTe enables federating to a degree that allows competing with big solution providers. Furthermore, without such seamless integration and interoperability, house operators and residents will potentially prefer being locked into a monopolistic solution provider, who is better able to ensure compatibility of all his proprietary smart home devices. Therefore, the next step for symbIoTe has to be compiling a sound line of arguments (not limited to the argumentation above) and action plan, with which small solution providers, house operators, and residents are convinced of symbIoTe.

The security tussle discussed in Section 4.2.2.3 showed that security of smart homes is safety relevant and also important to counter future DDoS attacks. This shows that the focus symbIoTe puts on security is justified and necessary and can be used as an additional argument to convince solution providers, house operators, and residents of symbIoTe.

4.2.3 Value Network Analysis

This use-case consists of three showcases (1) Healthy Indoor Air, (2) Smart Area Controller and (3) Active and Assisted Living (Smart Mirror). For each of the showcases an individual VNA was conducted. The initial VNA versions of the VNA graphs are based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the use-case partners were conducted to finalize the VNA's. In the following section a description of each VNA and its stakeholders can be found.

4.2.3.1 VNA for Show-case on Healthy Indoor Air

In the use-case Smart Residence, showcase (1) Healthy Indoor Air following stakeholders are consider in the VNA: *Home Automation Service Provider, AQ-Data Provider, symbIoTe, Weather Station Provider, Home Sensor Provider, Government, Resident*, and *Data Analysis Provider*. In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 2.

The interaction of the described stakeholders in Table 2 can be observed in Figure 19. SymbIoTe connects the air quality gathered by the *Government* with the *Data Analysis Provider* and the *Home Automation Service Provider's* platform. The *Data Analysis Provider* interpolates air quality data provided by the *Government* and based on the Residents location for a financial reward by symbIoTe in return. The Home Automation Service Provider's platform shares the residence location and home sensor air quality with symbIoTe. In return the interpolated air quality data gets provided to the *Home Automation Service Provider's* platform via *symbIoTe* for a payment. The *Home Sensor Provider* provides devices in return for a payment to the *Home Automation Service Provider's* platform. The *Resident* receives air quality data, alerts about air polution and quality, and advices, which result in a less polluted home and more efficient heating schedule, due to unnecessary venting. The *Resident* pays for the services provided by the *Home Automation Service Provider* and sets his system and air quality preferences in the providers platform. The *Government* funds Air Quality Data Providers for gathering data and knowledge about air quality. *Weather Station Provider* produce sensors and weather stations for the *Air Quality Data Providers* in return for financial rewards. Furthermore, the *Government* gets access to more air quality data from the home sensors as well as interpolated air quality data via *symbIoTe*.

Table 2: VNA Stakeholder description for UC Smart Residence - Healthy Indoor Air

Stakeholder	Description
symbIoTe	The intermediary platform to connect different home automation platforms with each other as well as open API's and service providers.
Resident	A homeowner with implemented home automation platforms in his home.
Home Automation Service Provider	Providing an IoT-Platform for various home automation purposes.
Home Sensor Provider	Provides sensors to the home automation platform.
Data Analysis Provider	Provides data analysis to other stakeholder connected to symbIoTe.
Government	European governments are required to collect air quality data[48].
Weather Station Provider	Manufactures the weather stations.
AQ-Data Provider	Gathers the air quality data captured by the weather stations.

symbIoTe connects different Home Automation Service Provider platforms with each other and enables further to have a unified interface to integrate other services i.e. Data Analytics Provider for interpolating air quality data.

Table 3: VNA Stakeholder description for UC Smart Residence - Smart Residence

Stakeholder	Description
symbIoTe	The intermediary platform to connect different home automation platforms with each other as well as apps and devices for controlling the smart home.
Resident	A homeowner with implemented home automation platforms in his home.
Home Automation Service Provider	Providing an IoT-Platform for various home automation purposes.
Things Provider	Provides sensors and devices with various applications to the home automation platform. This provider is of illustrative purpose and different providers are possible in real world.
Control App/Device Platform	Different interfaces for controlling the smart home devices. Software solutions as well hardware solutions are possible.

[48] According to the European directive 2008/50/EC [46]

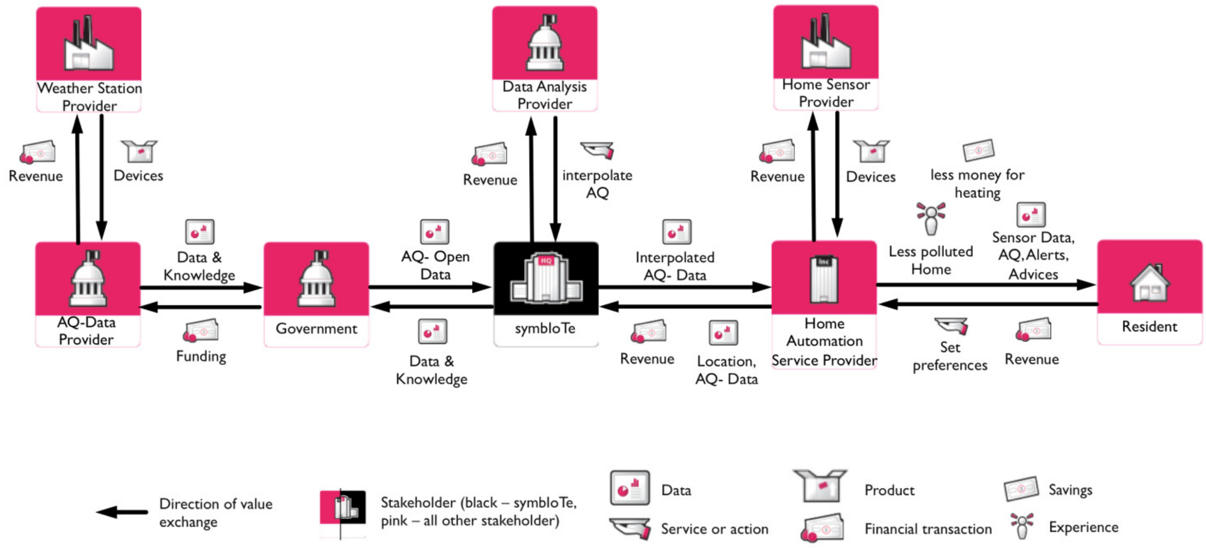

Figure 19: VNA Smart Residence, Show-case (1) Healthy Air [47].

4.2.3.2 VNA for Show-case on Smart Residence

In the use-case Smart Residence, showcase (2) Smart Residence (Smart Area Controller) following stakeholders are consider in the VNA: *Home Automation Service Provider, symbIoTe, Things Provider, Resident,* and *Control App/Device Platform*. In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 3.

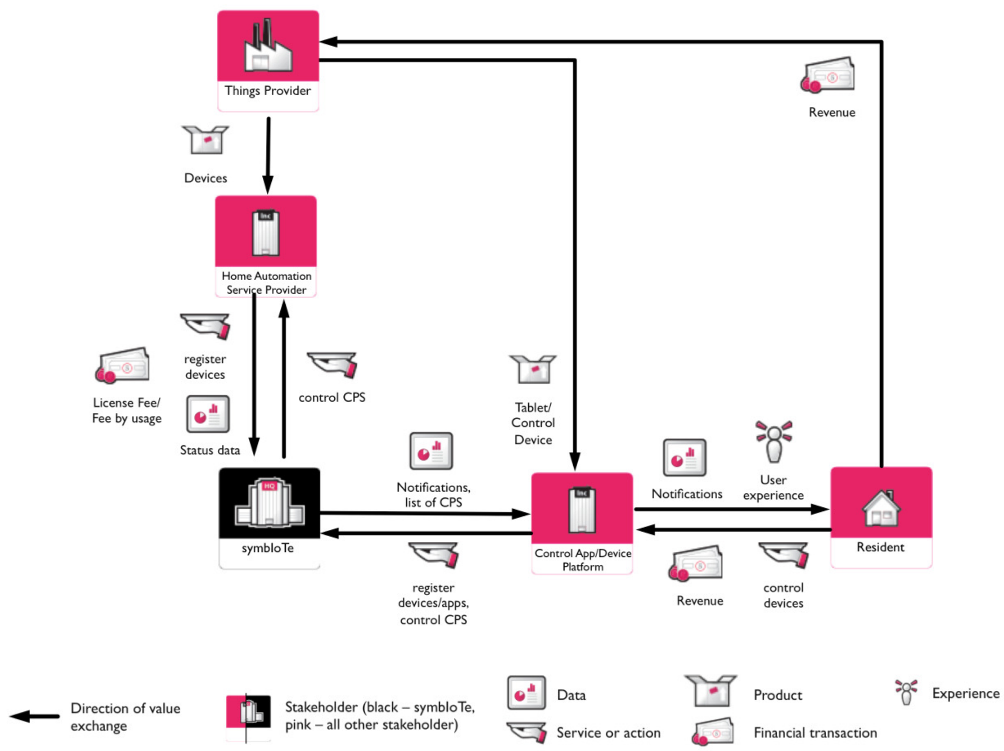

Figure 20: VNA Smart Residence, Showcase (2) Smart Residence [47]

Figure 20. The *Things Provider* provides devices to the *Home Automation Service Provider* as well as control devices to the *Control App/Device Platform.* The control devices could be i.e. thermostats, tablets or control panels. The *Resident* buys the devices for home automation from the *Things Provider* generating revenue as well as the control devices from the *Control App/Device Platform*. The *Resident* receives notifications and controls the home automation devices via the *Control App/Device Platform*. SymbIoTe connects the *Control App/Device Platform* with the *Home Automation Service Provider*. The *Home Automation Service Provider* registers and sends the status data of its devices to *symbIoTe,* which get forwarded to the *Control App/Device Platform*. Furthermore, the provider of the *Home Automation Services* has to pay a license fee or pay-by-use for the use of the *symbIoTe* services. The *Control App/Device Platform* registers all control devices and apps on *symbIoTe* and send the commands for controlling the cyber-physical systems (CPS) of the *Home Automation Service Provider*'s platform via *symbIoTe*.

The *Resident* experiences an enhanced user experience through a seemingless interaction with the smart home's different *Home Automation Service Providers*, which would require different user interfaces without *symbIoTe*.

4.2.3.3 VNA for Show-case on Active and Assisted Living

In the use-case Smart Residence, showcase (2) Active and Assisted Living following stakeholders are consider in the VNA: *Tele-health Platform Provider, symbIoTe, Resident, Physician, Caregiver, Activity Tracker Provider, Home Sensor Provider, Smart Mirror, Beacon Provider, Government, Medical Sensor Provider,* and *Health Insurance*. In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 4.

Table 4: VNA Stakeholder description for UC Smart Residence - AAL

Stakeholder	Description
symbIoTe	The intermediary platform to connect tele-health platforms with the smart mirror device.
Resident	An elderly homeowner in medical treatment and with a smart mirror at home.
Smart Mirror	A dedicated device for interacting with elderly residents in therapy.
Home Sensor Provider	Provides sensors for various measurements at home, i.e. scale, blood pressure monitor
Beacon Provider	Provides beacons or bracelets for identification of the resident (user).
Government	Government and European institutions, which provides product certifications and funding.
Tele-health-Platform Provider	Connects different institutions and stakeholders of the health industry with each other as well as with users.
Health Insurance	Insurer for residents, interacting with health personnel and tele-health platform provider in the process.
Caregiver	Health personnel taking care of people in an elderly home.
Physician	Health personnel doing therapy with patients.
Medical Sensor Provider	Providing professional medical sensors to the tele-health platform.
Activity Tracker Provider	Providing activity trackers, which are integrated into the tele-health platform.

Figure 21. The *Resident* can either be a user living at his own home or a elderly person living at a retirement home using the *Smart Mirror* and providing their measurements to it after receiving notifications and reminders. In case of living at a care center, the *Caregiver* buys the sensors of the *Home Sensor Provider* and the beacons for identification of the *Beacon Provider* and is setting them up at the *Resident's* room. In case of a *Resident* living at home, the *Resident* will buy and setup the sensors her-/himself. Activity trackers bought from the *Activity Tracker Provider* by the *Resident* allow to identify the *Resident.* The *Smart Mirror* registers all sensors connected to it on symbIoTe and sends a notification via *symbIoTe* to the tele-health platform once a measurement was taken. The *Smart Mirror has the possibility to look for already registered sensors and* receives a list of sensor URL from *symbIoTe*. The *Tele-health-Platform Provider* registers activity tracker identifiers for identification already in use at *symbIoTe* and subscribe for *Smart Mirror* measurement notifications. The *Physician* and the *Caregiver,* both part of the *Health Personnel,* setup the request for measurement on the *Tele-health-Platform* the request for data gets then directly forwarded to the *Smart Mirror*. The *Smart Mirror* sends the measurement data directly back to the *Health Personnel* via the *Tele-health-Platform*. The *Government (EU or national authorities)* in the European Union subsidizes the tele-health platform[49] partially as well as granting product certification to the tele-health platform as well as to the medical sensors provided by the *Medical Sensor Provider* and used by the *Tele-health-Platform Provider*. The *Health Insurance* subsidizes the *Tele-health-Platform* as well as the *Resident* for using the Smart Mirror as incentive for a healthy living and pays the *Health Personnel* for their services.

The benefit in the long term are better data on the resident's health and a reduction of unnecessary or belated doctor visits, which result in more grave consequences.

4.3 Use-case 2: EduCampus

This section analysis the EduCampus use-case by presenting a CANVAS analysis in Section 4.3.1, applying tussle analysis in Section 4.3.2, and finally conducting a value network analysis in Section 4.3.3.

4.3.1 CANVAS Use-case Owner View

In Deliverable D1.3 [15] the initial version of the CANVAS for the use-case EduCampus was presented. The CANVAS building blocks were filled with input available end of 2016. Within the last 1.5 years some changes in the use-case have occurred, so that a new iteration of CANVAS was necessary to illustrate the current state. This status is based on the input provided by use-case owners and contributors, as well as on available more detailed description of use-cases and their intended show-cases as described in Deliverable D5.2 [35].

[49] https://ec.europa.eu/health/ehealth/projects_en (last visit May 31, 2018)

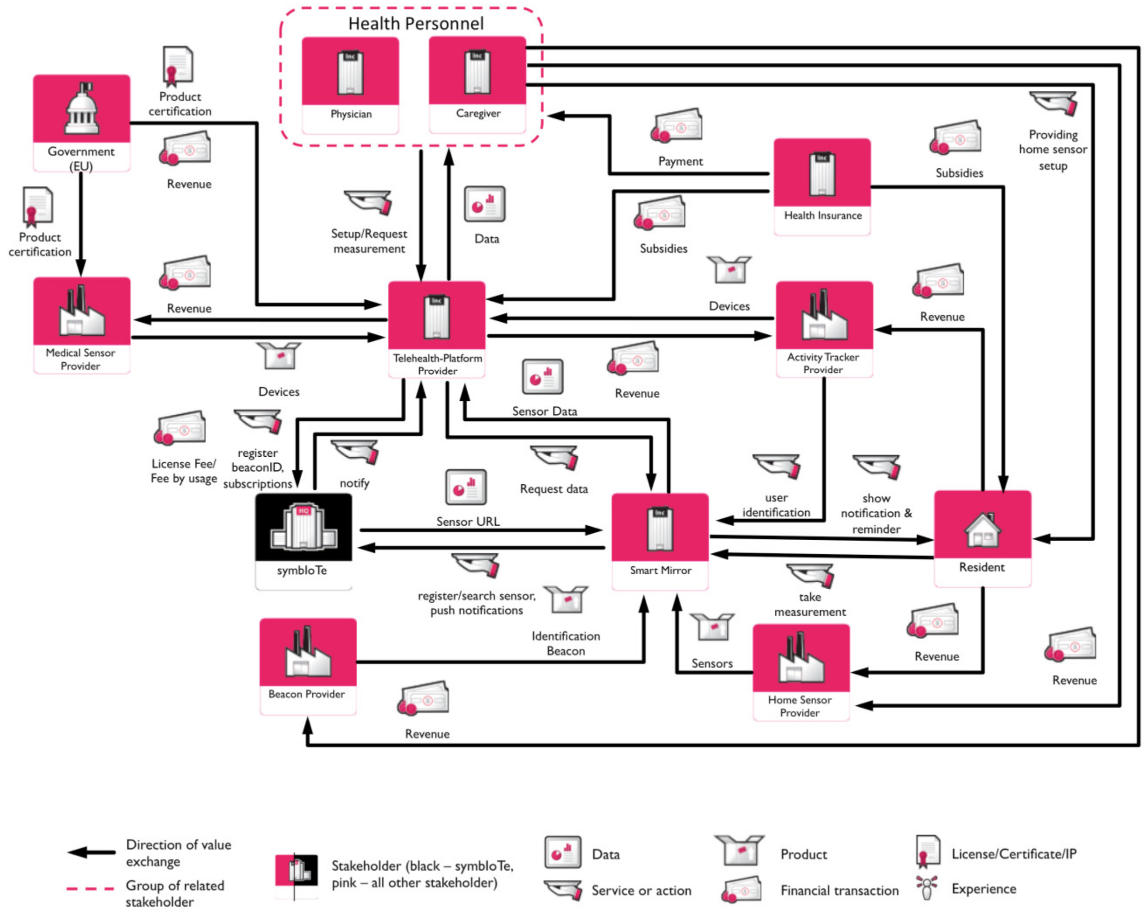

Figure 21: VNA Smart Residence, Show-case (3) Active and Assisted Living [47].

The involved partners decided as justified in Deliverable D5.2 [35] that the use-case EduCampus will cover two show-cases, namely (1) Campus Federation and (2) Third Party Services (e.g., catering). In the following for each of the show-cases a CANVAS is presented, but when putting them together in one global CANVAS it is obvious it matches the described initial version in [15]. The coloring is similar to the initial version: Yellow items have a general issue, green ones look on developer issues, and purple ones on customer related issues (here: University issues).

Show-case (1) Campus Federation describes alliance between different campus providers, by sharing room resources according to a common federation agreement, also known as service level agreement. The main purpose is to provide a better service to the campus users, like students searching for working places in partner sites, and at the same time safe administration costs by simplifying the registration of visiting campus users.

In contrast to show-case (1) the second show-case addresses the idea of third party involvement in a campus that can be triggered by events within the campus federation (e.g., convention, conferences, information evenings). A simple example for a third party involved in such events is a catering service. Thus, for the use-case EduCampus the intention is to interlink a service provider into the room registration service, in order to enhance the room and workplace service by an value added service to provide catering for meetings or even for personal needs (like the preferred coffee in the morning). This example is shown in the CANVAS in Figure 23.

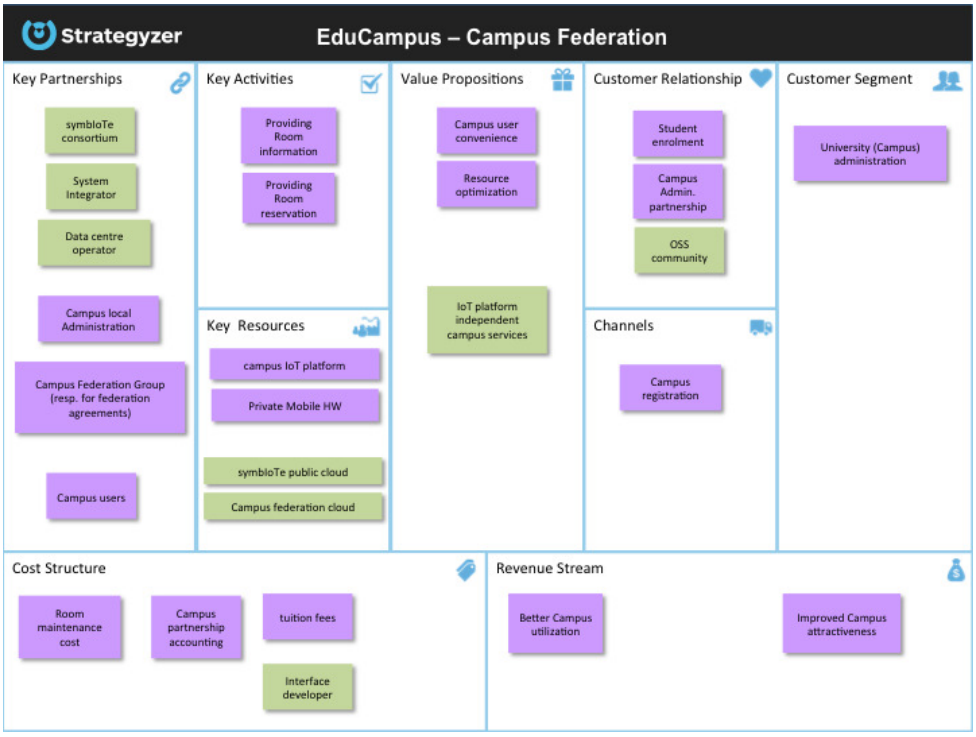

Figure 22: CANVAS for show-case “Campus Federation”

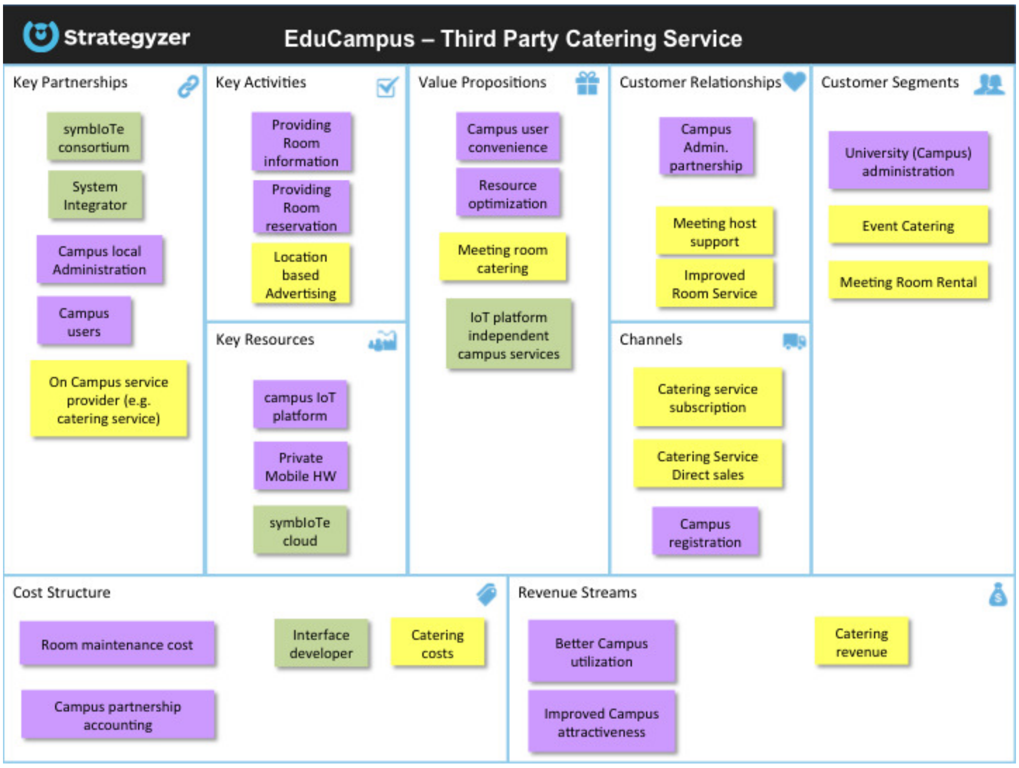

Figure 23: CANVAS for show-case “Third Party Catering Service”

Comparing both CANVASes with each other it is obvious that in all building blocks they have the following items in common: As key partnerships the symbIoTe consortium, system integrator, campus local administration, and the students using a campus environment were identified. The customer segment is in both the university (campus) administration. The revenue streams are the same, namely better campus utilization and improved campus attractiveness. As required key resources were in both the campus IoT platform and the private mobile hardware (e.g., smart phone, notebook, tabled) identified. The provisioning of room information and room reservation services was identified in both cases as key activities that goes hand in hand with the campus user convenience, the IoT platform independent campus service, and the resource optimization as identified value proposition items. The cost structure for sure includes in both cases the room maintenance costs and the campus partnership accounting. The campus partnership accounting includes all costs required to maintain the partnership within a campus federation. This may cover administration cost for visiting campus guests, maintenance cost for shared meeting or working place facilities, or compensation allowances for guest tutors and students.

The main differences can be found in the following building boxes, mainly due to the fact that the second show-case includes also customer related items (here: especially for the catering service assumed):

- Assuming a campus federation is in place as additional key partnership, a data center operator is required to maintain all information of participating campuses/universities and students that have the required credentials. From the administration point of view a campus federation group needs to be in place as well that is responsible for the federation agreements from legal and finance perspective. Those two new key partnerships are missing in the second show-case because they are irrelevant, due to the fact that catering is assumed to happen only on one campus at given time. Hence, an “on campus service provider” (e.g., catering service) needs to be added here.
- For the second show-case also location-based advertising was identified as an additional key activity to announce the special event a third party is involved in.
- From the key resources perspective both have a cloud in place, but distinguishing between a public and private cloud depends on the specific requirements of a given deployment solutions Furthermore, show-case (1) generally requests a campus federation cloud, because a campus independent resource discovery service is required. On special agreements within a given federation, other deployment strategies are possible, like the hosting of common services within a selected campus provided data center.
- For show-case (2) an additional value proposition was identified related to the offered service (here meeting room catering) of the third party.
- The customer relationship identified for show-case (1) is the Open Source Software (OSS) community. In comparison the meeting host support and improved room service was identified for the second show-case instead.
- In show-case (2) additional channels were identified such as catering service subscription and direct sales that are directly linked to the offering third party service.

- The customers segment is extended by event catering and meeting room rental for the show-case (2).
- Based on the third party service the cost structure needs to be adjusted with catering cost and with tuition fees for campus federation, respectively.
- Revenue streams got expanded with the item catering revenue for the second show-case.

4.3.2 Tussle Analysis

The EduCampus use case aims to simplify the life of students, by providing interoperability between student IDs and by simplified room bookings and even friend finding services via an app. In the process also managerial costs can be reduced. For example, by being able to use a student identity also during a semester abroad, less identity cards have to be issued. However, this reduced managerial cost for students and campus administrations also means reduced revenues for the companies issuing the cards. Section 4.3.2.2 discusses this very generic tussle, which is not unique to the symbIoTe solution but arises generally, when processes are made more efficient and, thereby, allow to cut costs. Section 4.3.2.3 also discusses a generic tussle: the need that a user provides information that can be used to increase services offered to him but also abused in different ways. Section 4.3.2.4 highlights implications that these tussles have for the next steps to be undertaken by the symbIoTe consortium. Before the discussion can begin, Section 4.3.2.1 lays the ground by identifying all involved stakeholders and their interests.

4.3.2.1 Stakeholders and Interests

Deliverable D1.3 [15] identifies the stakeholders campus administration, campus users, and campus service providers. The campus administrations aim to lower the administration costs and to improve the campus user experience. Campus users also aim to reduce their spendings (mainly by tuition fees) and appreciate access to a great variety of digital services, such as friend finding and room booking via smartphone applications. Campus users are mainly students and, therefore, subsequently referred to as such. Campus service providers sell services such as burrowing books and printing services and want to maximize these sells or rather the revenue through these sells. A stakeholder not mentioned in D1.3 but relevant for this tussle analysis are ID card providers. They are companies that provide the identity management and room access system (this includes providing student identity cards) to the universities and make revenue from selling these services. Table 5 summarizes the stakeholders and their interests.

Table 5: Stakeholders and their interests for the EduCampus use-case.

Stakeholder	**Interest**
Campus administration	Decrease administration costs, increase student satisfaction
Students	Decrease spendings, conveniently access variety of services
Campus service providers	Increase their service sells
ID card providers	Increase their ID card sells

4.3.2.2 Adoption Tussle

This tussle is generic for the socioeconomic paradigm of the industrialized world, as incompatibilities often increase revenue streams. More precisely, inefficiency often results in the possibility to make greater gains for some stakeholder. In this concrete use case the inefficiency on the students' site is the inability to use his university ID card at different universities. Therefore, if a student moves to another university he has to acquire a new card, which is often associated with a fee. This cost may be hidden to the students, when the card provider charges the university for the provided cards. The university will cover these costs by the tuition fees. Therefore, the ID card providers have an interest to maintain this inefficiency, as it allows them to collect more fees. Furthermore, integrating an automated solution will come with extra cost in terms of hiring specialists who integrate this technology. Therefore, the ID card providers have no incentive to conduct a costly process that will decrease their ability to sell their services/goods. Therefore, the symbIoTe solution has to be pushed by the universities themselves. In particular, the campus administration has to cover the cost for integrating this solution. Also it may be necessary to contract a different ID card provider, if the current one is not willing to adopt the symbIoTe solution. All this implies significant overhead and costs for the campus administrations. An advantage that the symbIoTe solution offers to universities is the reduction of administrative overhead. However, this advantage will likely only be sufficient to compensate for the additional overhead and costs in case of campus federations (in this case, students will be exchanged very frequently between campuses). Therefore, such campus federations have to be directly approached by the symbIoTe consortium, to make them aware of and support symbIoTe. Furthermore, students, who are the main beneficiaries of the symbIoTe solution, have to be mobilized to support the adoption. In particular, students directly benefit from the symbIoTe solution by a simplified guest registration and more flexible workplace management. To mobilize students, those benefits have to be clearly demonstrated to them, for example, by giving demonstrations to bodies representing students and their interests. Also campus service providers that provide value added services, like catering together with room booking, through the symbIoTe solution should be mobilized to urge universities to adopt the symbIoTe solution. The symbIoTe solution will also make it easier for students pay for printing or borrow books. Therefore, campus service providers offering these services will also see increasing revenues and should be mobilized to support the adoption of symbIoTe.

4.3.2.3 Location Privacy Tussle

After the adoption tussle is solved successfully, the symbIoTe solution will provide location-based services such as friend finding or ad-hoc room reservation. However, the student location (required by these services) is also very valuable to campus service providers and other marketers to make, e.g., location based advertisements, which may degrade the symbIoTe solution to an advertisement platform that benefits marketers more than students.

To overcome this tussle, it is important that a student can control who has access to which information about the student. For example, a student must have the possibility to grant a friend-finding service access to his location, such that he can be shown friends in his proximity. At the same time, the student must be able to hide this information from campus service providers, as they may flood the student with push notifications, when he gets near their locations.

4.3.2.4 Implications for symbIoTe

The adoption tussle discussed in Section 4.3.2.2 showed that symbIoTe has to overcome the resistance of already established stakeholders to establish itself in the market. Furthermore, initial investment costs that are necessary to deploy symbIoTe may render an obstacle for bringing the symbIoTe solution to the market. To maximize symbIoTe's chances of making it to market, the support of the right stakeholders has to be sought: the first stakeholders are university administrations. Here, university administrations of universities, which are part of campus federations and, therefore, exchange students with high frequency, are best suited to be approached. In particular, if universities exchange students frequently the eased administration of students moving between campuses may easily outweigh the initial costs of adopting symbIoTe and, therefore, approaching universities, which are part of a campus federation (e.g. [31,32,33]), is most promising. The second stakeholder to seek support from, are campus service providers, as they may be able to increase their sells by offering their services through the symbIoTe solution. Accordingly, also these stakeholders have to be made aware of the advantages symbIoTe offers, so they support symbIoTe's adoption. This convincing of campus service providers is most likely achieved, by presenting them with concrete numbers on how they can increase their sells through symbIoTe. The last stakeholder that should be convinced of the symbIoTe solution are campus users, as they will directly benefit from the convenience symbIoTe offers. As students constitute the largest percentage of campus users, an example is to approach student representations in order to make them aware of the advantages symbIoTe offers. In subsequent interactions with campus administrations, these student representations are then expected to voice their interest of adopting the symbIoTe solution. Student administrations and other campus users are probably best convinced of symbIoTe by demonstrations of symbIoTe's functionality.

Accordingly, the next step to be undertaken by the symbIoTe consortium is developing a concept of how each of these three stakeholder groups can be best convinced. This plan should include very specific arguments as well as presentation material (tailored to each of the stakeholder groups) and ways of how to approach the stakeholders. An argument that will be important to university administrations and campus users is that the symbIoTe solution will allow campus users to control, who can access their location. The relevance of this functionality was identified, when analyzing the location privacy tussle in Section 4.3.2.3.

4.3.3 Value Network Analysis

The use-case EduCampus is based on the initial definitions in deliverable D1.3 [15] and additional information provided by D5.2 [35]. Further input provided by the involved partners was used to complete the initially designed VNA by the end of March 2018.

As mentioned in Section 4.3.1 the use-case EduCampus consists of two showcases: showcase (1) Campus Federation and showcase (2) connecting third-party services to the campus platform. Both of these use-cases are reflected in one VNA (cf. Figure 24).

The stakeholders involved in the value network of the EduCampus use-case are Campus User, Home Campus Platform, symbIoTe, Admin of University, 3rd Party Infrastructure Provider, 3rd Party Service Provider, Home University, and Partner University. In order to understand the role of each stakeholder in the value network a short description is provided in Table 6. The stakeholder list in context of the VNA is considering previously proposed stakeholders by the CANVAS and TA, but amended the list to fit the perspective of the VNA. Thus, some stakeholders are excluded, but other stakeholders are included.

In order to highlight the benefit of symbIoTe as a federation platform two universities are part of the VNA as shown in Figure 24. A Home University and a Partner University, former is shown in a higher granularity to reflect the value network within one university campus. In the first showcase the actors involved in one campus are Home Campus Platform, Administration of University, and Home University. Within the campus the Administration of University provides administration services via the Home Campus System to the whole network and its Campus User's, these include: Discover/Offer Services, Request cooperation, Negotiate SLA, Process Campus Affiliation Request, as well as authenticate user access requests. In return they receive the necessary data to perform their services. The Home Campus Platform gets funded by the Home University itself and provides data and knowledge about the campus to the university. For the Home University the work for campus user access verification from Partner Universities as well as from other campus within the same university gets reduced. Furthermore, the effort to access other collaborative services between two universities, which previously had to be handled individually by the administration, decreases, due to a common interface. Thus, the university reduces spending on its administration.

Table 6: VNA Stakeholder description for UC EduCampus

Stakeholder	Description
symbIoTe	The intermediary platform to connect different universities, campuses within universities and third-party service providers.
Campus User	A campus user is a person eligible to use the campus network and infrastructure, i.e. a student of this university, a guest student, a professor, a guest professor or any kind of member of a federated partner.
Home Campus Platform	The it-platform as interface for symbIoTe of the university providing the campus services to students, professors, and employees.
Administration of University	Handles all back office requests and tasks, which include access authorization and setting up third party service contracts.
Home University	Resembles the head of the home university or university board, which handles all financial aspect and take decisions.
Partner University	Resembles the partner university as a whole with all actors shown in the home campus included.
3rd-Party Infrastructure Provider	Provides sensors and devices for the IoT-Platform of the university.
3rd-Party Service Provider	Provides the services for the second showcase i.e. catering or suppliers for gadgets or tools used in booked rooms.

The Home University buys sensors and devices from 3rd-Party Infrastructure Providers, which get integrated into the Campus Platform. These gather and provide information about the rooms, i.e. room temperature, or beacons for localizing the campus user. The Home Campus Platform forwards the administration services and room information to the symbIoTe platform, which provides the data to the Partner University. The Home Campus Platform in return receives the data and services from the partner university via symbIoTe. The two universities benefit further from a better collaboration between each other. The partner universities fund their share of the symbIoTe platform.

The Campus User pays his tuition fee to the Home University and gets, after sharing his location and credentials, access to the Home Campus Platform. The platform shares information about the Home University as well as the Partner University with the user. The Campus User will always connect to the Home Campus Platform independent from its location, home campus or at the Partner University.

The second showcase is based around the 3rd-Party Service Provider, which gains access to symbIoTe by paying a fee to the university where they are located. The services they provide are then registered on symbIoTe and made available to the Campus User, i.e. when booking a room. This process decreases the workload of the Administration of University further since offers and services have not to be organized by them anymore. Complementary services are organized and agreed on by the Campus User as requester of the service. Therefore, the Campus User has to pay the agreed price for the booked services. How expenses are handled within the university and its Campus User is out of scope of this VNA.

The above described processes will ultimately result in less administrative work and costs by a simplified registration and campus access process for visiting Campus Users. Providing access to administration services for home-based as well as for visiting Campus User, reduces administration effort and cost further. The integration of 3rd-Party Service Provider allows the direct arrangement between the campus user as a requester and the provider. Therefore, taking the Administration of University out of this process decreases their workload additionally.

4.4 Use-case 3: Smart Stadium

This section analysis the Smart Stadium use-case by presenting a CANVAS analysis Section 4.4.1, applying tussle analysis in Section 4.4.2, and finally conducting a value network analysis in Section 4.4.3.

4.4.1 CANVAS Use-case Owner View

In Deliverable D1.3 [15] the initial version of the CANVAS for the use-case Smart Stadium was presented. The CANVAS building blocks were filled with input available end of 2016. Within the last 1.5 years some changes in the use-case have occurred, so that a new iteration of CANVAS was necessary to illustrate the current state. This status is based on the input provided by use-case owners and contributors, as well as on available more detailed description of use-cases and their intended show-cases as described in Deliverable D5.2 [35].

Technically speaking, the offering may vary depending on the amount of platforms involved, as reflected in the Value Network Analysis. For this reason, the initial business model CANVAS has been split into three smaller ones, called showcases, in order to reflect the differences in the value proposition and customers involved. Those are (1) visitor application, (2) retailer application, and (3) promowall application. For all CANVAS the following color scheme is assumed: Purple entries are issues related to citizens, green entries are issues related to developers, and yellow entries indicate general issues.

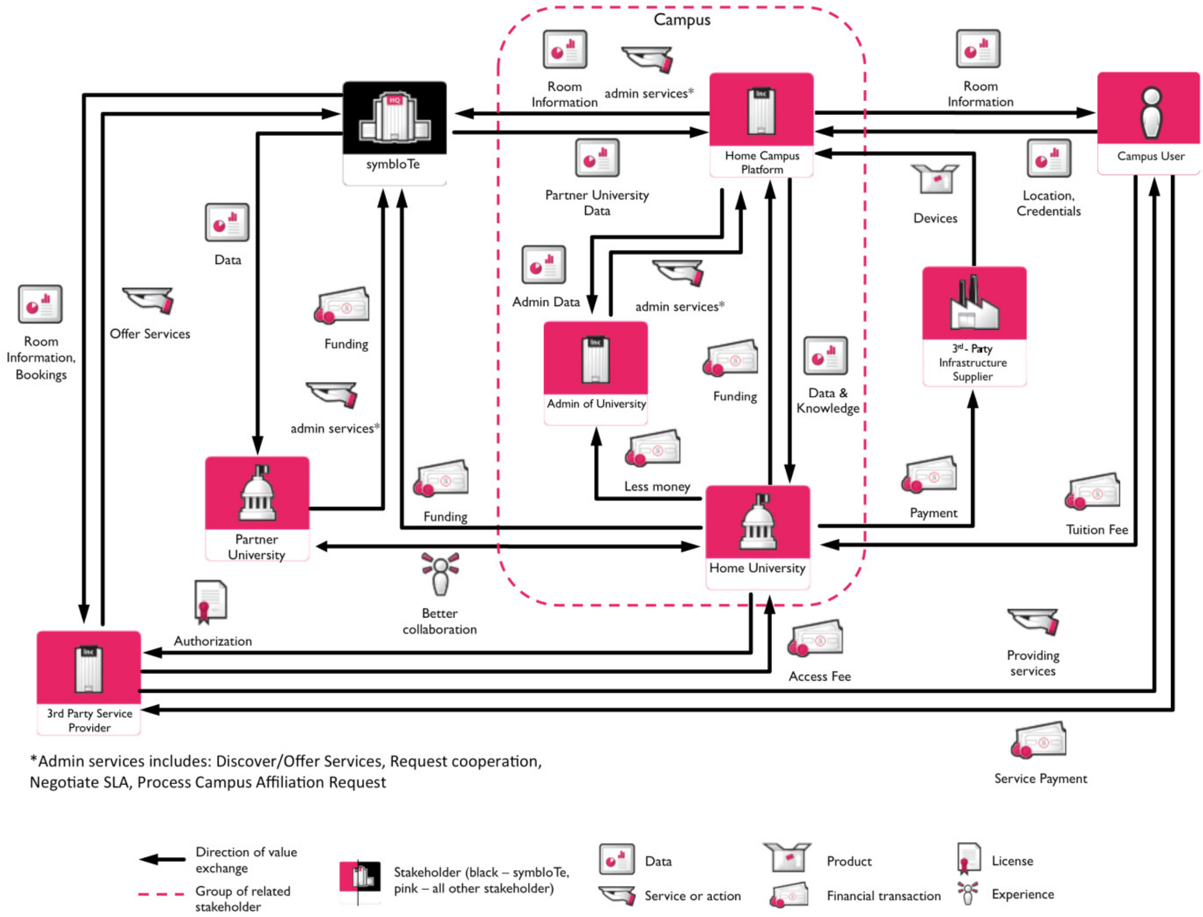

Figure 24: VNA EduCampus [47]

The **visitor application** applies to smart indoor routing, aiming to improve the visitors' experience when attending to any event within an enclosure area. Whenever there is an event in any of these places, a huge amount of people is expected to attend. For this people the stadium offers a set of services located in different zones. This showcase focuses on buying/selling goods. Sometimes attendees want to buy some food or souvenirs from the existent shops, but they are not aware of their location. Atos Worldline aims to offer a smart routing service for them.

Figure 25 shows the CANVAS developed for this showcase. As key partnerships IoT platform owners, cloud service providers, data providers, and symbIoTe offering owners were identified. Due to the fact that the planned use-case will handle many sensitive data that include personal information a further stakeholder must be mentioned here, namely legislative organizations dealing with the GDPR (General Data Protection Regulation) [37] enforced May 25, 2018. The focus of the UC Smart Stadium is on events taking place in sport stadiums, and thus, stadium owners and operators are the target customer segment here, as well as public/private entities (i.e. Public Administrations organizing any kind of social event in the stadium, such as benefit concerts, or private musical or party promoters who can make use of the sport facilities under a certain fee) and the visitors as end users. Hence, dedicated assistance at customer level is identified to establish long-term customer relationship, such as human interactions with customer representatives' or making use of automated services, i.e. customized services per customer or any other onsite communication (e-mail, call center). Resulting in a successful application, three main key activities were identified: (i) Integration and extension of services/infrastructures providing, and improving, full user experience (i.e. suggestions based on each customer preferences), (ii) service innovation and evolution of symbIoTe-based services (i.e. nearest places or best routes that weren't available before), and (iii) customer engagement (i.e. developing and offering new services to be deployed in the stadium at a lower cost). The required key resources are mainly linked to ATOS, the UC owner, and include symbIoTe L1 (interoperability) and L2 (federation), connected assistance, integrated and full value added user experience, sales force & customer base, experiences from past events (e.g., as the main IT provider for Olympic and Paralympic games from Barcelona 1992 to PyeongChang 2018), and mobile app and IoT devices. As channels to publish the showcase own channels from ATOS are envisioned to be used in marketing and sales portals, as well as face-to-face meeting with clients. Based on all those building blocks mentioned the cost structure is quite complex and includes items like technology development, marketing, business development, installation and maintenance of hardware/software, hardware associated costs, and human resources costs. In order to cover these costs different revenue streams are envisioned like monthly fee, pay-per-use, commercialization with third parties, and data analytics. If everything is in place and the application is running successfully, the following items are envisioned as value proposition: Addition of on-demand rapid and flexible value services such as designing faster evacuation routes and alternatives, not initially contemplated, integration with different IoT platforms as each stadium manages its own platforms which expose different APIs, efficient data management coming from sensors and smart devices, enhanced services for stadium operations based on the integration of different underlying platforms, and on-demand services (e.g., smart routing) based on the available data.

The **retailer application** is an evolution of the previous one. Bearing in mind users cannot only look for the nearest shop or cart, but to do some reservations in advance for certain goods. As an example, a visitor aims to buy a specific item and looks for the nearest shop through the mobile application. Visitor goes to the shop but the item is not in stock, now he has to wait for it to be delivered or move to another shop, losing time and probably attendance to the event. Within this showcase, the visitor will be able to do a reservation in advance, what allows the shop to first check if the item is in its stock and, in case it is not, to order it to another shop within the stadium. If this is not possible, the user can look for another shop. This is not only beneficial for the user but also for the shops, which are now able to increase their selling during the event.

The related CANVAS is shown Figure 27. As it can be seen mainly everything is the same all over CANVAS's building blocks, because this offering is built on top of the previous one. The visitor cannot only make a reservation but do it in the nearest shop to save time. The only exceptions can be found in the customers segment targeted and in the intended value proposition, where both building boxes are extended by one item each. In the target customer segment retailers need to be added to the group of end-user, because they are the main stakeholder target here. Here the visitors are still mentioned, because they are the ones doing the reservation in one specific shop. In value proposition the on-demand services offered are expanded further by a reservation item for retailers, because now they have the opportunity to interact on one hand with the user, who is doing the reservation, and on the other hand with other shops, in order to ensure that the appropriate item will be in stock prior to the customer visit.

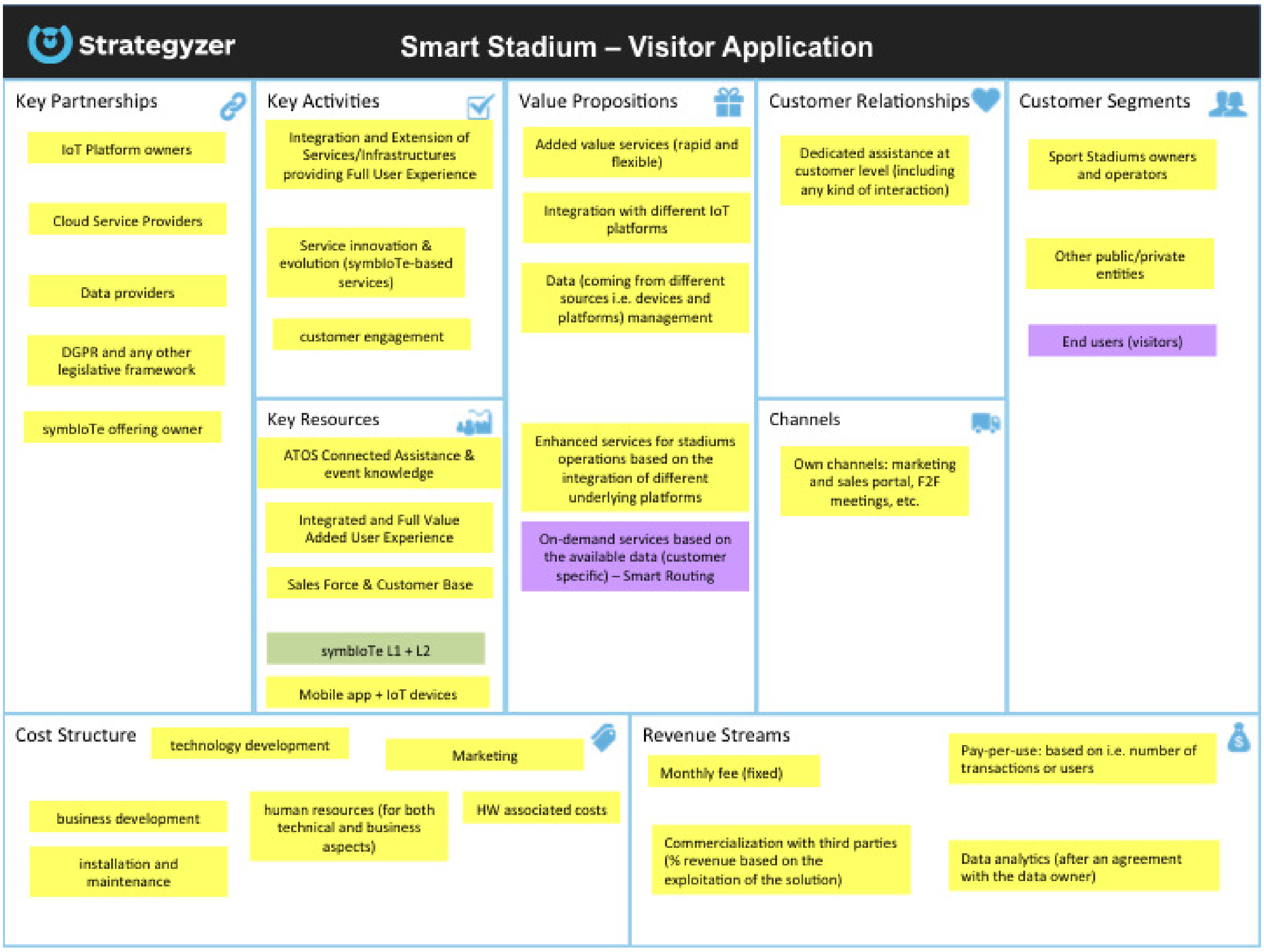

Figure 25: CANVAS for visitor application of UC Smart Stadium

Within the **promowall application**, the user is not only able to find the best route or to do a reservation but to benefit of discounts in any shop. A third platform is used here, installing promowalls in different locations within the stadium. Offers are displayed in the promowalls and the user can scan them to get coupons, these coupons will be later on redeemed at the shop to get discounts on the items that will be bought. The related CANVAS is shown in Figure 27 and as it can be seen it is the same as in the retailer application case, but includes a further on-demand service in the value proposition case, namely smart offering. This include things like smart routing and smart reservation in order not to only get a discount but to get it in the nearest shop ensuring that the item will be available before the customer arrives.

4.4.2 Tussle Analysis

symbIoTe's goal for the smart stadium use case is the improvement of the communication between visitors' devices and the stadium infrastructure, to improve visitor experience and sells inside the stadium. In particular, the Smart Stadium use case describes three main functionalities: (i) routing of users through the stadium via an app, (ii) displaying of offers in the app or promowalls, and (iii) preordering goods via the app. After Section 4.4.2.1 has introduced the main stakeholders and their interests, each of the functionalities is examined for tussles in a separate section. Section 4.4.2.5 rounds off the discussion by highlighting implications that the tussle analysis has for the next steps to be undertaken by the symbIoTe consortium.

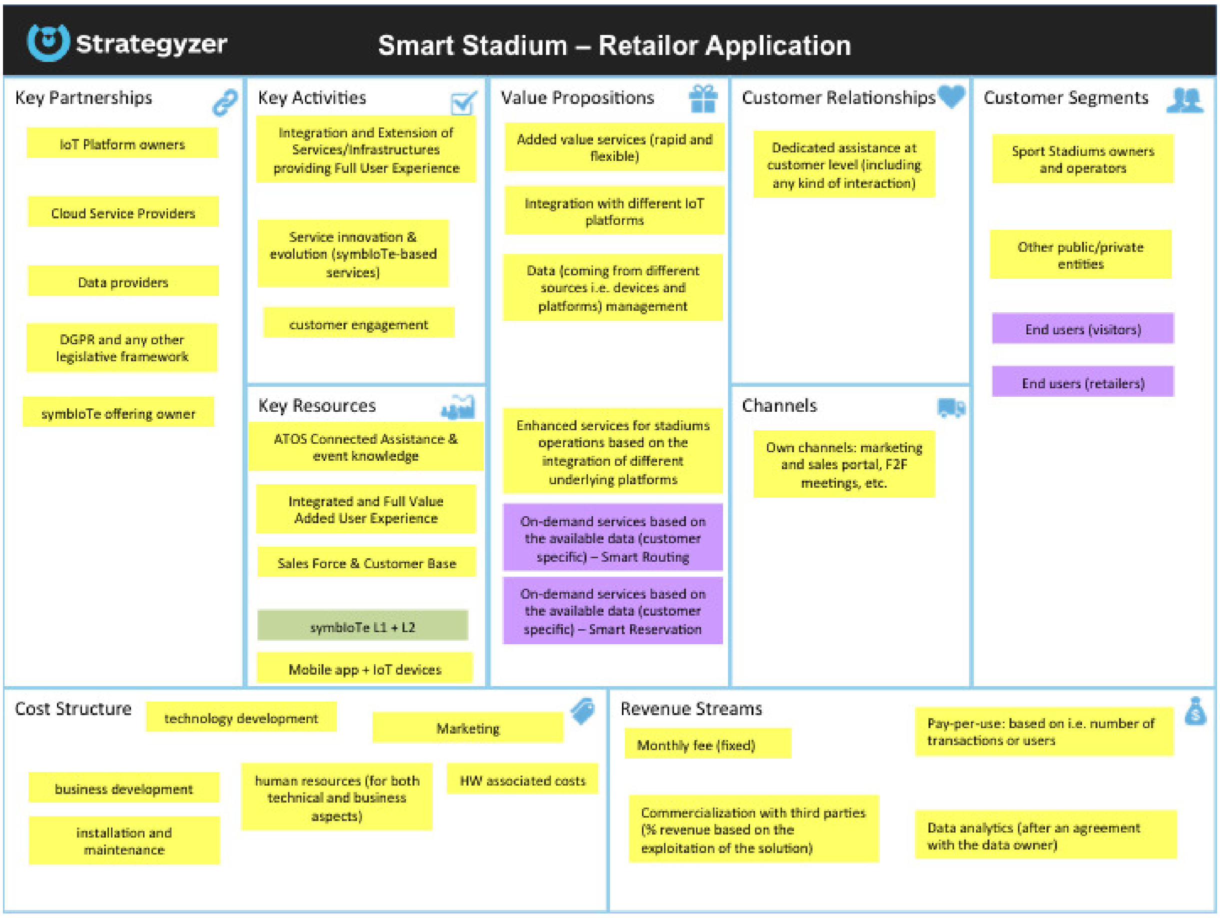

Figure 26: CANVAS for retailer application of UC Smart Stadium

4.4.2.1 Stakeholders and Interests

The Smart Stadium use case sees the following three stakeholders. The stadium manager operates the stadium and wants to maximize revenues. Revenues come not only from selling stadium tickets but also from renting out booth places to retailers or by participating in the revenues they make. The selling of tickets implies that a secondary interest of the stadium manager is maximizing the experience of visitors. However, a maximized visitor experience does not necessarily imply the maximization of the stadium manager's revenues. Retailers sell their goods and services in the stadium to visitors. Also they want to maximize their revenues, which equates to maximizing their sells. Visitors want to have a pleasant experience inside the stadium whereat this experience has to be in proportion to the money they spend. This experience is influenced by how available different services inside the stadium are and how easy it is to navigate inside that stadium (a visitor that gets lost inside the stadium may have a significantly impaired experience). Table 7 summarizes the stakeholders and their interests.

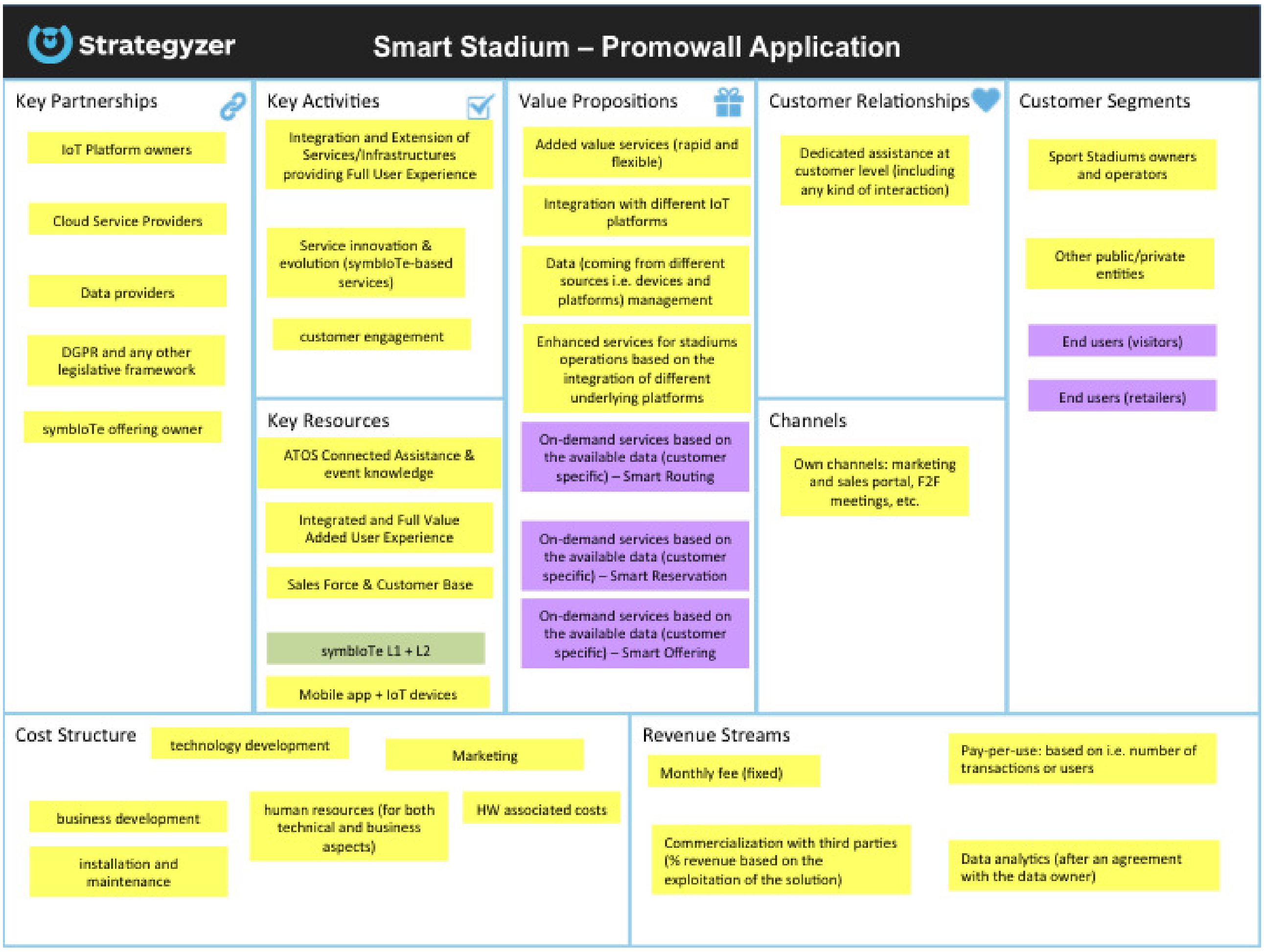

Figure 27: CANVAS for promowall application of UC Smart Stadium

Table 7: Stakeholders and their interests of the Smart Stadium use case

Stakeholder	Interest
Stadium manager	Maximize revenues, i.e., ticket sells and fees collected from retailers
Retailers	Maximize revenues, i.e., sells
Visitor	Have pleasant and affordable experience

4.4.2.2 Displaying offers

The interests of different retailers to sell their goods and services collide. However, this does not constitute a tussle, as it qualifies as desired market-based competition. A new element in this competition is the advertisement of the retailers' offers on the visitors' phones and promo walls. In particular, retailers will be able to increase their sells, when their offers are displayed prominently. The stadium manager is the stakeholder who controls this display of offers. Therefore, the symbIoTe system gives the stadium manager control he did not have before. However, also this does not constitute a tussle. The reason is that the stadium manager has to provide a fair playing field for all retailers (in order to not lose them) and, therefore, should either display all offers in neutral order or give all retailers the opportunity to improve their display rank by payments. The latter would even create an additional revenue stream for the stadium manager.

In order to increase the relevance of displayed offers, the symbIoTe solution allows displaying offers through the app based on the visitors' location. This implies that the visitors share their location with the app. As location based displays can be sold at a higher price to retailers and location based displays have higher chances of resulting in a purchase, the stadium manager profits from visitors sharing their location. Therefore, the stadium manager has incentive to maximize the app experience, when visitors share their location with the app. This ensures that the stadium manager does not abuse the visitors' location for "location based spamming" and generally tries to maximize the app experience. For visitors, who do want to share their location with the app, the following more conservative approach is possible: these visitors can share their seat-number with the app. The seat number tells the stadium manager in which part of the stadium the visitor is located but not the precise, real-time position. Therefore, sharing the seat number with the app constitutes a good tradeoff between user privacy and precision of location-based offerings.

4.4.2.3 Preordering

The app will allow visitors to preorder items and subsequently pick them up. This preordering has to be associated with some kind of identity, such as social network account or credit card information. If preorders were not associated with an identity, retailers could flood competitors with preorders that are never paid, thereby, harming competitors' business. The identity to be provided requires a login and may change from stadium to stadium. However, credit card information is best suited, as it allows for prepayment of orders.

4.4.2.4 Routing of Users

Sells of retailers increase, when visitors are routed inefficiently through the stadium. In particular, visitors, who would have gone directly to their destination, may make spontaneous purchases, when routed by according opportunities. The stadium manager, who provides the routing information, profits from the sells made by retailers in the stadium. The reason is that the stadium manager either directly collects a certain percentage of the retailers revenues or he rents the booth places to retailers. In the latter case, he will still profit from increased retailer sells, as it allows increasing booth prices in the future. Therefore, the stadium manager has incentive to route visitors via detours along retailers.

Some visitors may appreciate these additional opportunities for purchase, while other visitors may not. This renders a tussle between the stadium manager and visitors who want to take the shortest path. This tussle can be simply mitigated by providing a map of the stadium to visitors through the app. In particular, this makes routing transparent to the visitors by providing them sufficient information to verify that they are indeed routed along the shortest path or make autonomous routing decisions. Therefore, it is recommended that a stadium manager increase transparency and trust by providing a map of the stadium, which will not only prevent this tussle but also be helpful for many other purposes. Furthermore, visitors should be offered to select "shortest path" or "purchase friendly" routing, since some visitors may be in a rush while others appreciate additional opportunities for purchase.

4.4.2.5 Implications for symbIoTe

Adopting new software or hardware on a large scale always implies initial, additional costs. Therefore, the stadium manager, who is the key stakeholder to adopt symbIoTe and has to pay these costs, has to be certain that the additional long-term revenue enabled by the symbIoTe solution outweighs the initial costs of adopting it. Such additional revenue can easily be expected, when looking at the functionalities that symbIoTe offers in the smart stadium context: the displaying of offers makes visitors more inclined to make purchases, which increases revenues of the stadium manager. More importantly, the displaying of offers even creates a new revenue stream for the stadium manager, as discussed in Section 4.4.2.2. The possibility to preorder items at retailers makes purchasing easier (cf. Section 4.4.2.3) for visitors and is, therefore, also be expected to increase the stadium manager's revenue. Lastly, also the purchase-promoting routing, as discussed in Section 4.4.2.4, has the potential to increase sells inside the stadium and, therefore, the stadium manager's revenue.

Accordingly, there are several strong arguments for a stadium manager to deploy the symbIoTe solution. Thus, the next steps for the symbIoTe consortium are to compile these arguments into a convincing presentation and approach stadium managers, seeking their support. Here it is important to highlight advantages over competitor's solutions (if such competitors exist), for example by stressing the new revenue stream that location-based offerings through the app create.

4.4.3 Value Network Analysis

This Use-case consists of three showcases (1) Visitor Application, (2) Retailer Application and (3) Promowall. For each of the showcases an individual VNA was conducted. The initial VNA versions of the VNA graphs are based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the Use-case owners were conducted to finalize the VNAs. In the following section a description of each VNA and its stakeholders can be found.

4.4.3.1 VNA for Visitor Application Showcase

In the Smart Stadium use-case, showcase (1) Visitor Application the following stakeholders are consider in the VNA: Visitor(s), Stadium Manager, Network Infrastructure Provider, symbIoTe platform (more likely L1 and potentially L2), Sensor/Beacon Platform, Smart Stadium Provider, and Retailer. In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 8.

All of the described stakeholders are part of the VNA in this show-case (cf. Figure 28). In order to highlight the benefit of the symbIoTe platform in this showcase, the whole network gets described starting with the *Visitor*. The *Visitor* downloads the Smart Stadium application and registers himself. By accepting the agreement, the Visitor provides his/her location within the smart stadium. Whenever the *Visitor* looks for a product, he does it through the downloaded application. In return the *Visitor* receives the location of close services provided by retailers and shops, as well as routes to these locations. A transaction between a *Visitor* and a *Retailer* takes place once the *Visitor* is at a retailer store and receives a product or service in exchange for a payment. The *Retailers* register their services and offers on the symbIoTe platform. They will then get forwarded to the Smart *Stadium Provider*'s platform. The symbIoTe platform available within the stadium can be operated by the *Smart Stadium Provider* or a third party provider. Depending on the case a license or maintenance fee must be paid. Further content information about the

Retailers will get provided to the *Smart Stadium Provider's* platform directly. The *Stadium Manager* is providing license to the *Retailer's* for operating their businesses within the stadium in return for a license fee. The *Stadium Manager* pays *Sensor/Beacon Platform* provider to add sensor and beacons to the symbIoTe platform. The *Stadium Manager* is contracting a *Network Infrastructure Provider* to provide sufficient connectivity to the *Retailers* and *Visitors* since regular mobile network would be overloaded with the number of devices trying to access the services.

Table 8: VNA Stakeholder description for UC Smart Stadium - Visitor Application stakeholders' description

Stakeholder	Description
symbIoTe	The intermediary platform to connect retailers with the smart stadium platform and the sensor/beacon platform.
Visitor	People visiting the stadium for a game or another event and is in possession of a smart phone with the smart stadium application.
Stadium Manager	Is in charge of the stadium operations and allowed to file contracts with retailers and other stakeholders.
Network Infrastructure Provider	Provides connectivity to all stakeholders within the stadium.
Sensor/Beacon Platform	Different providers of sensors and beacons with different platforms, all of which get connected to the symbIoTe platform.
Smart Stadium Provider	The stadiums own information platform, which acts as interface for the visitor and handles all the services.
Retailer	Is a retailer located in the stadium providing his services or/and sells his products/goods to the visitors.

These processes allow the *Visitor* to connect to the Smart Stadiums systems and offered services through one interface independently of the platforms the stadium uses. Beacons and sensors for registering the *Visitor's* and *Retailer's* location are registered on the symbIoTe system to get accessed by the *Visitor* through the *Smart Stadium Provider*'s platform.

4.4.3.2 VNA for Retailer Application Showcase

The second showcase for this use-case is the (2) Retailer Application. The stakeholders are the same as for the (1) Visitor Application showcase. Thus, the same stakeholder description is valid as shown in Table 8. Since the stakeholders are the same some relation between the stakeholders stay the same. However, there are relations, which are affected compared to the first showcase, namely *Retailer-symbIoTe, Retailer-Smart Stadium Provider,* and *Smart Stadium Provider-Visitor.*

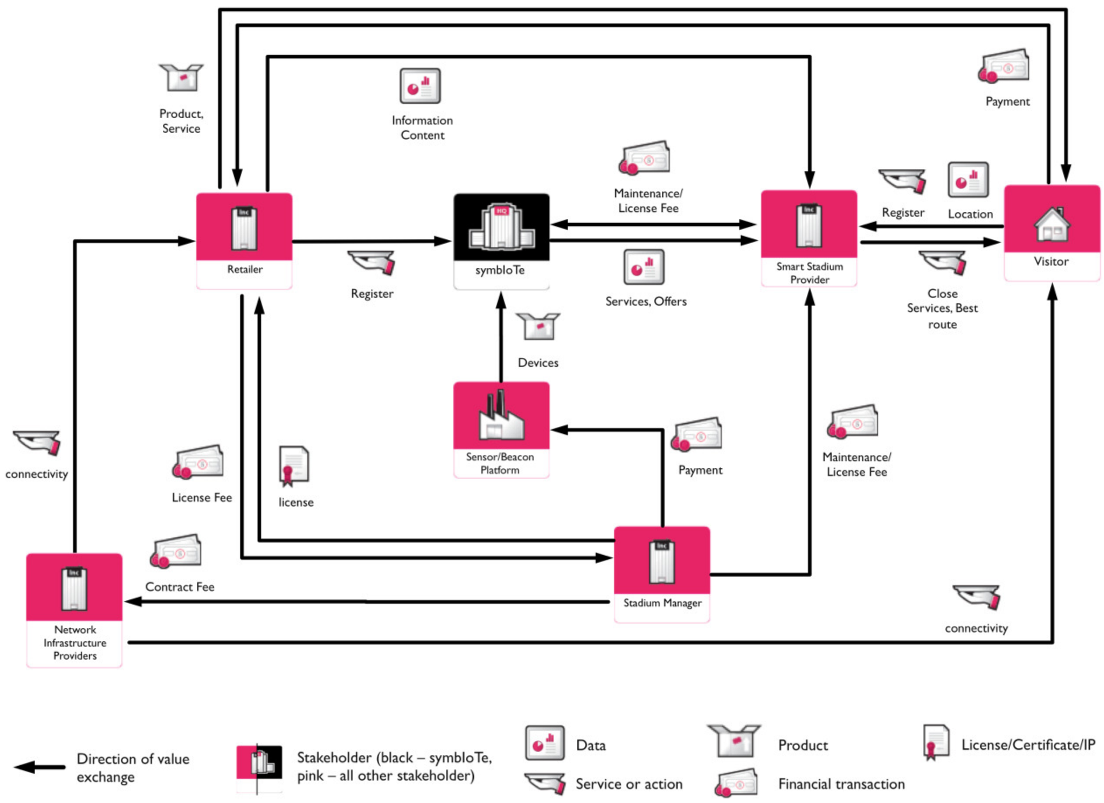

Figure 28: VNA Smart Stadium, Show-case (1) Visitor Application [47]

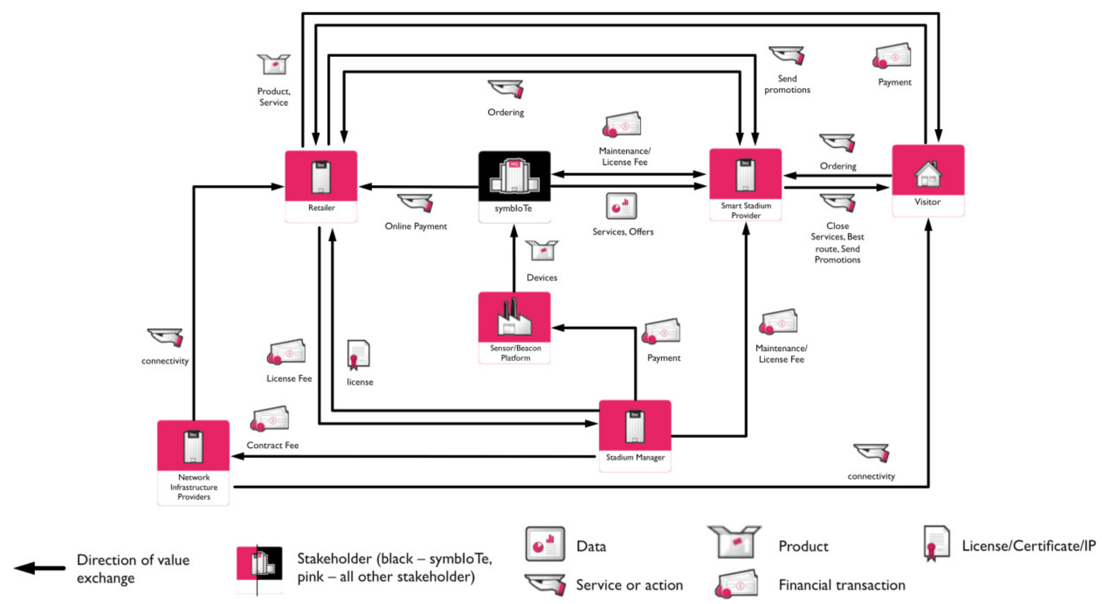

Figure 29: VNA Smart Stadium, Show-case (2) Retailor Application [47].

The remaining relations of the first show-case and the named relations are reflected in Figure 29. The focus lies on the *Retailer's* interactions initiated through the ordering process performed by the *Visitor*. The application of symbIoTe reduces the complexity of setting up the *Retailer’s* services and makes the interaction with the stadiums IT-infrastructure easier. The registered services and offers provided by the *Retailers* get provided to the *Visitor* as well as the close services, and best routes to the *Retailer’s* shop. The *Retailer* sends as well promotions to the *Visitor* via the *Smart Stadium Provider’s* platform. The orders placed by the *Visitor* on the *Smart Stadium* Provider get forwarded directly to the *Retailer.* The *Retailer* can as well order services and offers through the *Smart Stadium Provider’s* platform. Furthermore, the symbIoTe platform enables the Online Payment. Although this feature is not yet available, it is a nice to have one. In order to allow payment online, it is necessary to have a payment gateway that it is not available in this moment. The use of symbIoTe as the middleware platform for interconnecting other platforms simplifies the inclusion of a payment one, managed by a third party, and to develop the additional services in the final application.

4.4.3.3 VNA for Promowall Application Showcase

In the third showcase of Smart Stadium Use Case, the (3) Promowall Application, the list of stakeholders is the same as in showcase (1) Visitor Application, but is complemented by the *Promowall platform*. For a better understanding of the role the *Promowall* plays, a stakeholder description can be found in Table 9.

Table 9: VNA stakeholder description for UC Smart Stadium - Promowall stakeholder description

Stakeholder	Description
symbIoTe	The intermediary platform to connect retailers with the smart stadium platform and the sensor/beacon platform.
Visitor	Visits the stadium for a game or another event and is in possession of a smart phone with the smart stadium application.
Stadium Manager	Is in charge of the stadium operations and allowed to file contracts with retailers and other stakeholders.
Network Infrastructure Provider	Provides connectivity to all stakeholders within the stadium.
Sensor/Beacon Platform	Different providers of sensors and beacons with different platforms, all of which get connected to the symbIoTe platform.
Smart Stadium Provider	The stadiums own information platform, which acts as interface for the visitor and handles all the services.
Retailer	Is a retailer located in the stadium providing his services or/and sells his products to the visitor.
Promowall platform	The platform connects all the Promowalls and provides the functionality to send promotions and coupons to the Promowalls.

The interactions of described stakeholders (cf. Table 9) in the Promowall show-case are shown in Figure 30. The interaction between the *Visitor* and the *Promowall platform* through the Promowall and his smartphone allows the *Visitor* to capture promotional coupons. The promotions and coupons presented on the Promowalls are sent by the *Retailer* to the *Smart Stadium Provider’s* platform and from there forwarded to the *Promowall platform* via symbIoTe. Offerings linked to the promotions are presented to the *Visitor* directly from the *Smart Stadium Provider’s* platform on the smartphone. Depending if the *Smart Stadium Provider* is operating the symbIoTe platform itself or if a third party is operating the symbIoTe plattfrom there either has a license or maintenance fee to be paid. For the captured coupons the *Visitor* receives discounts on the product when redeemed by the *Retailer*. The *Retailer* gains exposure through increased visibility of its services by the loss leader. The result of the increase interactions between the *Visitor* and Stadium's infrastructure increases the attractiveness for further promotions and advertisement on the Promowalls. This in return enables an increase in license fee revenue for the *Stadium Manager* paid by Retailers for their advertisements.

The relations of the *Network Infrastructure Providers*, *Stadium Manager* and *Sensor/Beacon Provider* are the same as in show-cases (1) Visitor Application and (2) Retailer Application. Thus, a description of these relations can be found the respective sections.

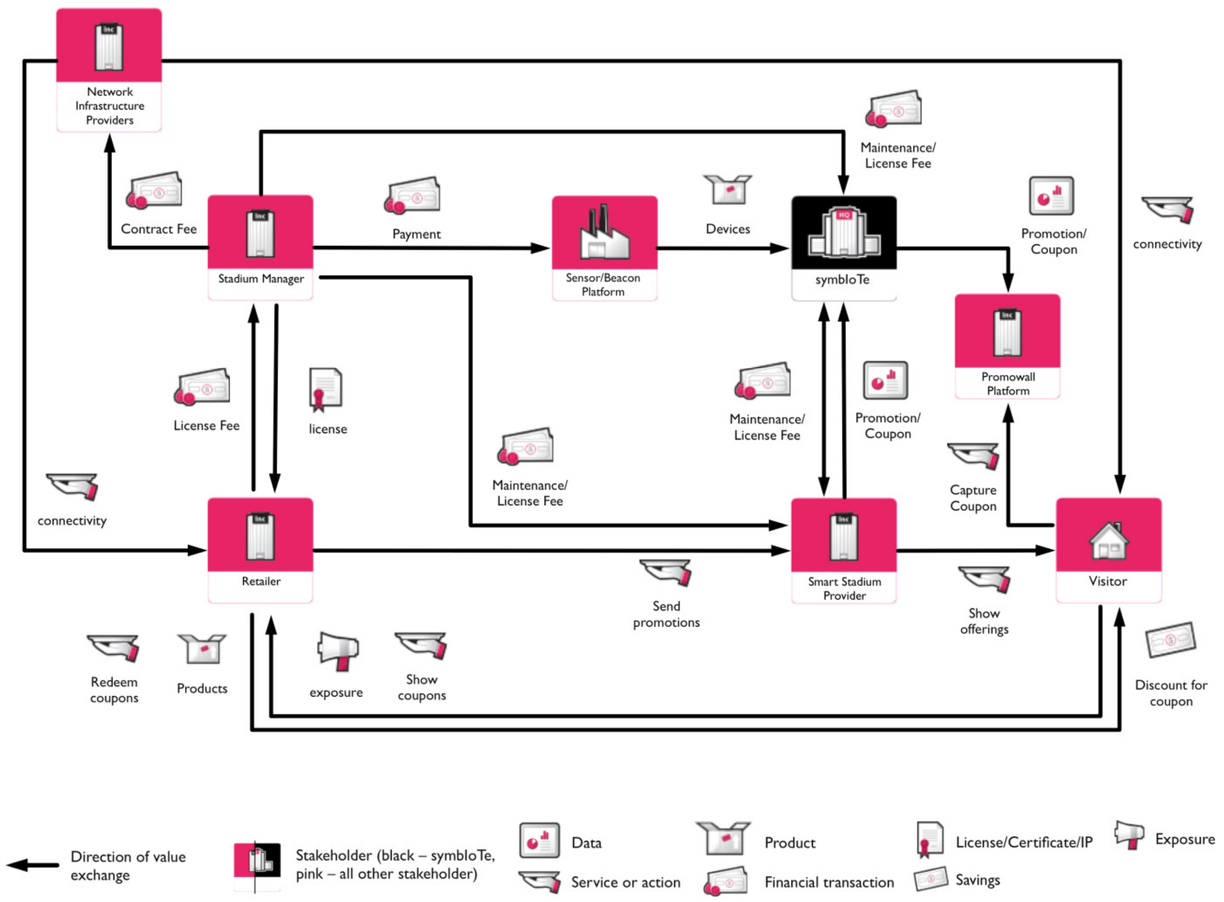

Figure 30: VNA Smart Stadium, show-case (3) Promowall Application [47].

4.5 Use-case 4: Smart Mobility and Ecological Routing

This section analysis the Smart Mobility and Ecological Routing use-case by presenting a CANVAS analysis Section 4.5.1, applying tussle analysis in Section 4.5.2, and finally conducting a value network analysis in Section 4.5.3.

4.5.1 CANVAS Use-case Owner View

In Deliverable D1.3 [15] the initial version of the CANVAS for the use-case Smart Mobility and Ecological Routing was presented. The CANVAS building blocks were filled with input available end of 2016. Within the last 1.5 years some changes in the use-case have occurred, so that a new iteration of CANVAS was necessary to illustrate the current state.

This status is based on the input provided by use-case owners and contributors, as well as on available more detailed description of use-cases and their intended show-cases as described in Deliverable D5.2 [35].

The use-case "Smart Mobility and Ecological Routing" aims on addressing the problem of inefficient transportation and poor air quality that many European cities face nowadays. This use case will offer the ecologically most preferable routes for motorists, bicyclists, and pedestrians based on the available traffic and environmental data acquired through multiple platforms. For air quality monitoring, the data obtained by in-situ environmental monitoring stations can be combined and enriched by the data readings collected by wearable sensors and mobile devices (the mobile crowd sensing approach) to provide enriched environmental measurements, which are dense both in space and time. At the same time, the routing planner takes mobility information, such as traffic measurements related to road traffic congestion and parking spaces occupancy offered by fixed sensors, as input data for the ecologically preferable route calculation.

The resulting CANVAS is shown in Figure 31 assuming the following color scheme: Purple entries are issues related to citizens, green entries are issues related to developers, and yellow entries indicate general issues. The identified key partnerships include the symbIoTe consortium as a provider on the platform itself, mobility services and municipalities as target audience, as well as hardware providers and device manufactures for needed equipment. In comparison the customer segments also include sports industry, app developers, citizens, collective transportation providers, and green users (people who want to use applications that allow for a more sustainable lifestyle) that all would benefit form the idea of ecological routing. To satisfy the stakeholders, it is important to focus on the essential key activities such as up-to-date algorithms, data analysis, geolocalization, and route planning. Those need to be combined with partners' engagement and will incorporate the parking availability, because the use case does not focus on a single group of users, rather it aim at providing a generic services for all types of users present in urban areas including those that have to park their vehicles (e.g. including bicycles). For a successful implementation of the use-case key resources are essential; identified are already IoT resource discovery and access, semantic interoperability, domain and routing enablers.

The latter two are represented by anyone developing applications on top of symbIoTe (e.g., for Zagreb and tourism: http://www.betherezagreb.com/ plus add/incorporate in here routing service provided by symbIoTe enabler). Based on those building blocks the resulting customer relationships are online platform customer service, customer support channels, partnership establishment, and open source development community. Channels used for connections are social networks, direct sales, online subscription, demonstrations, partners' websites, and the project website. Having those blocks in place the cost structure can be specified having five main items in place, namely business development, technical infrastructure, marketing, research & development, and human resources. With the right revenue streams (e.g., advertising, subscription plans, license fees) the cost become affordable to build a good value proposition. The value proposition envisioned for this use-case can be divided into

- Citizens related issues like convenience, general support of CO_2-reduction, rewards for providing air quality data, health improvement, and mobility integration, and
- Developer related issues such as IoT platform / 3rd party interoperability, enablers, Cloud based solutions, and open source frameworks.

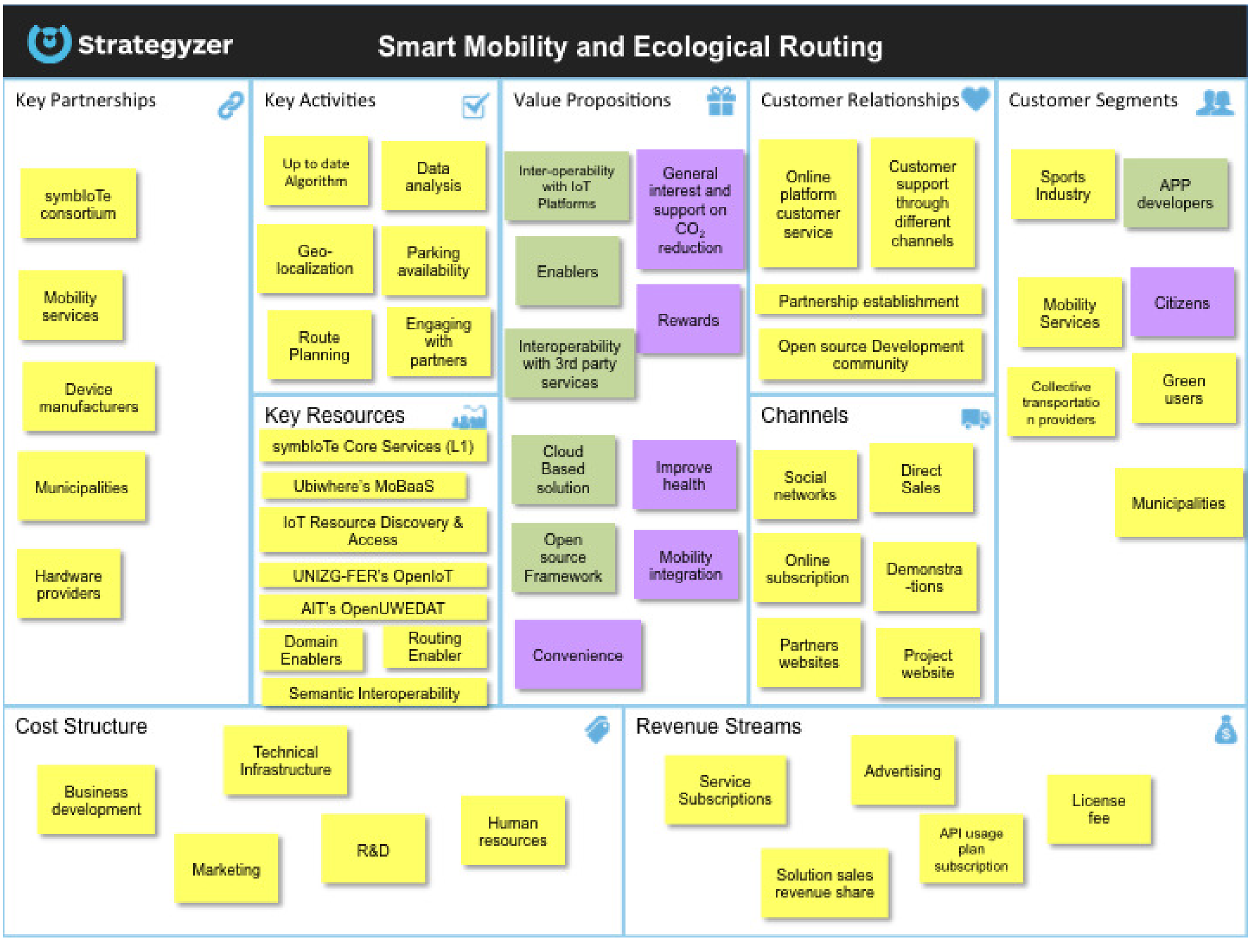

Figure 31: CANVAS for use-case “Smart Mobility and Ecological Routing”

4.5.2 Tussle Analysis

The Smart Mobility and Ecological Routing use case aims at gathering environmental data from user devices and fixed stations and, based on this information, suggest routes and Points of Interest (PoI) to the individuals. Three tussles are identified for this use case. The first tussle is discussed in Section 4.5.2.2 and reveals that incentive have to be provided to commercial IoT platform providers to support symbIoTe. How this incentive is to be provided is currently an open question. The second tussle arises around the guidance of individuals (“guidance” means routing and/or PoI suggestions), as misguidance of individuals allows sellers (such as restaurants and shops) to make a significant financial gain. This tussle is discussed in Section 4.5.2.3. The third tussle arises because the symbIoTe solution aims at incorporating data provided by end-user devices but the gathering and provision of this data decreases battery life. This tussle is discussed in Section 4.5.2.4. Section 4.5.2.5 highlights key findings from these three tussles and resulting questions to be answered by the symbIoTe consortium. Next, Section 4.5.2.1 provides the discussion ground for subsequent tussles by identifying all relevant stakeholders.

4.5.2.1 Stakeholders and Interests

Table 10 summarizes all stakeholders and their interests discussed in this section. “Supposed to” in the column “Interest” indicates that the stakeholder is supposed to be neutral. However, employees of that stakeholder may try to profit from behaving in a non-neutral manner. This special case is not considered further.

Individuals are involved in every tussle of this use case. The interests of individuals are to have a high degree of privacy, in terms of location traceability. Also they want to save battery life and have good guidance information, i.e., routing and PoI information that is calculated from a large set of correct measurement data. Measurement data is provided by individuals' wearable devices and fixed stations. Sellers are also a prominent stakeholder group for this use case and include businesses such as restaurants. Their interest is to maximize their revenue, which is increased by more guests. In turn, the number of guests can be increased in multiple ways. Examples are having more individuals walk by their location, or rank higher in the recommendation system. Sellers rank higher, when they are able to report advantageous environmental data from their location, or by bribing data aggregators. Data aggregators aggregate all measurement data to reply to individuals' requests. Therefore, data aggregators are in a very powerful position and, thus, should be neutral bodies such as governments. The data to be aggregated by data aggregators is sourced from different IoT platforms. These IoT platforms can provide aggregation services themselves and exchange data with other IoT platforms through symbIoTe. Therefore, the interest of IoT platform providers is gathering high quality data and trading this data with other IoT platforms in exchange for their data. Fixed station operators are a special case of IoT platform providers. Fixed stations provide measurement data just as individuals' wearable devices do. However, the measurements provided by fixed stations are usually of higher quality, as these stations have no energy of size constraints.

DDoS attacks performed by criminals are also an issue for this use case. As explained for the Smart Residence use case in Section 4.2.2.3.1, criminals can attempt to make revenue by blackmailing. However, in the smart mobility use case DDoS attacks are fundamentally different, as they are not digital but physical. In particular, criminals can provide false information through the system to route individuals along the same traffic junction, effectively congesting this junction. When emergency cars frequently use this junction, this becomes a serious issue for the common wealth.

Table 10: Stakeholders and their interests of the Smart Mobility and Ecological Routing use case.

Stakeholder	Interest
Individuals	Privacy, battery life, good guidance information
Sellers IoT platform providers	Maximize revenue, i.e., increase visiting individuals Gather measurement data to monetize it
Data aggregators	*Supposed to* provide correct aggregation results
Criminals	Blackmailing by DDoS attacks
Fixed station operators	Gather measurement data. If run by a city, this gathering may not be revenue oriented

4.5.2.2 Adoption Tussle

SymbIoTe is envisioned to collect environmental data from different IoT platforms and use this data to guide users. Therefore, the question arises, what incentive IoT platform providers have to provide their data to symbIoTe. While academic or research driven IoT platforms, such as OpenIoT, openUwedat, and MoBaaS, are expected to provide their data for free, commercial IoT platform providers will want to monetize the data they gather by selling or trading it. This raises two questions:

1. **How can commercial IoT platform providers be compensated for providing data to symbIoTe?** If this question cannot be answered, commercial IoT platform providers cannot be expected to provide data to symbIoTe or even support it protocol wise.
2. **How can commercial IoT platform providers be prevented from inventing data?** This question is relevant, (a) when looking at the trading of data between different IoT platform providers through symbIoTe, as well as (b) when looking at the provision of data to symbIoTe. The question is relevant in both cases, because an IoT platform provider has to be compensated for sharing data. Unfortunately, providing artificially generated data will also increase the compensation. Therefore, an IoT platform provider has incentive to "invent" measurement data to increase his compensation.

Subsequently, it is assumed that these questions are successful answered and, therefore, the adoption tussle is solved.

4.5.2.3 Guidance (Routing and PoI Suggestion)

In this use case symbIoTe is deployed to guide individuals ("guidance" means routing and/or Point-of-Interest suggestions). How an individual is guided through the physical world critically determines the individual's decisions and how the individual affects the world. Accordingly, this guidance-functionality of symbIoTe can be greatly misused and/or monetized and, thus, bears potential for tussles.

Guidance tussles can be distinguished in two dimensions: 1) the information that is falsified (either routing or Point-of-Interest suggestions) and 2) the means used to falsify it (either through spoofing measurement data or by bribing the data aggregator). Subsequently, these aspects are discussed individually and findings summarized in Table 11.

Table 11: Summary of the guidance tussles.

	Falsify	
What?	Routing information	PoI suggestions
Why?	Increase Guests, reroute traffic, perform physical DDoS	
	Means	
Spoof	Measurements	Aggregates
How?	Trick or emulate sensors	Bribery
Prevention	IDs	Non-profit aggregator
Problems	Miscalibrated sensor, bulk misreporting, privacy loss	PoI ranked high independent of individual preferences

4.5.2.3.1 Falsifying Routing Information

Stakeholders who can profit from tempering with the routing of individuals are amongst others sellers. For example, a coffee shop with tables on the sidewalk has incentive to reduce traffic in front of it to offer guests a nice and calm atmosphere. Alternatively, restaurants profit when more individuals (by car or foot) pass by as this increases the number of potential guests. However, also more futuristic exploits are possible: rerouting cars or pedestrians can be exploited for real-world DDoS attacks. For example, a street or crossroad can be jammed, when a sufficient number of cars are routed along it. This is particularly critical, if emergency vehicles frequently use the street or crossroad. However, here the exploiting stakeholders are not sellers but criminals, who blackmail cities with DDoS attacks.

4.5.2.3.2 Falsifying PoI Suggestions

Altering PoI suggestions can be misused to increase the number of customers of sellers. In particular, a seller will usually profit from being prominently displayed as suggested PoI. However, similar to the real-world DDoS attack outlined above, PoI suggestions can also be misused to overload a seller with customers, similar to a flash mob.

Routing information and PoI suggestions can be falsified by two different means, as discussed next.

4.5.2.3.3 Spoofing Measurement Data

PoIs are suggested by the symbIoTe solution based on different environmental information, such as air quality data or noise levels. This information is collected from fixed stations, as well as, end-user devices. Fixed stations are usually under the control of the government or a company and, therefore, can be considered trustworthy. However, end-user devices are less controllable and can, therefore, be used to report false data. Notably, it may not even be necessary to own an end-user device but it may be sufficient to emulate end-user devices and misreport data with these virtual devices. Such misreporting may, for example, give a restaurant an unfair competitive edge: Most restaurants benefit from increasing their reported air quality data and decreasing their reported noise levels, as this is what is perceived as pleasant and comfortable by most individuals. Therefore, they will rank higher as PoI according to the search criteria of most individuals. However, pubs may profit from increasing reported noise levels, as it suggests a more lively and crowded pub. Either way, it is clear that sellers significantly benefit, if they are able to alter environmental data reported about their location. Therefore, sellers have incentive to emulate devices or place real devices in artificial environments to spoof environmental data.

Spoofing of data can be aggravated by the use of IDs. IDs allow comparing data reported by IDs that are currently nearby each other. If data reported by an ID constantly deviates from the average reported, it is likely that this ID reports wrong information. Accordingly, the data reported by this ID should be discarded and the ID blacklisted. However, there are three problems with this solution: firstly, data reported by an ID may stem from a falsely calibrated sensor and not malicious intents (however, one may argue that it is good to block miss-calibrated sensors). Secondly, if a seller emulates several misreporting sensors, a correctly reporting sensor entering the seller's premise may be falsely classified as malicious. And thirdly, associating measurement data with an ID makes users easy to trace. In particular, due to the geo-tagging of data movement patterns of users become easily traceable. This third problem is very generic, as usually a tradeoff exists between data authenticity and user privacy, which can be summarized as follows: To guarantee validity of data/measurements they have to be associated to a user identity, which collides with privacy concerns.

To further mitigate the problem of misreported data symbIoTe is also investigating the introduction of a "trust factor" for every sensor. This trust-factor will be determined automatically for every sensor based on statistics about its deviation from the reporting of nearby sensors. Finally, this factor determines how much the reporting of an individual sensor is factored into the final aggregated result.

4.5.2.3.4 Aggregation Result

Just as users can be "lured" to or away from certain PoIs or routes by the provision of false measurement data, this also can happen, when the data aggregator alters the aggregation results. In particular, restaurant owners have incentive to bribe an aggregator in order to guide users in their favor. This way of falsifying the results has a decisive advantage: when the data is spoofed, routes or PoIs can only be made attractive to a group of individuals with certain preferences. For example, by reporting a restaurant as quiet, it will rank higher for individuals looking for a calm place. However, it will not rank higher for individuals looking for a lively and therefore, louder place. By falsifying the aggregation results, however, a restaurant can be displayed prominently to all individuals, independent of their preferences.

Therefore, the neutrality of the data aggregator is of critical importance. Commercial companies have financial interests and are, therefore, not well suited for the role of the data aggregator. In contrast, governmental bodies can be viewed as non-profit organizations and are therefore less prone to bribery. In particular, governmental bodies may still be bribed, however, this corruption then stems from a subgroup of individuals within that body and not the profit orientation of the company as a whole.

This tussle illustrates a general problem: stakeholders that aggregate large amounts of data and reach a large number of individuals with the results have high impact and, therefore, can make large financial gains, when being bribable or altering the aggregates in a non-neutral manner. Non-neutrality in such cases may have to be prevented by judicial interventions. A good example for this is [34].

4.5.2.4 Battery Life Tussle

The tussle subsequently described is an instantiation of a common dilemma and not caused by symbIoTe. Therefore, symbIoTe currently does consider it out of scope and does not develop mechanisms to address it. However, due to its generic nature, it is worth being discussed nonetheless.

This use case envisions that environmental data is collected via end-user devices. Collecting data from end-user devices compared to fixed stations offers the advantage that data will be collected in varying locations and that end-user devices greatly outnumber fixed stations. Unfortunately, collecting data via end-user devices decreases the battery life of these devices and battery life is the most pressing issue for many mobile users. Therefore, individuals' desire for long battery life collides with the common interest of having diverse measurement data, which increases the quality of information provided to everyone. As this is a conflict of interests, it qualifies as a tussle. Interestingly, the stakeholders whose interests collide are actually the same: on the one hand, end-users want routing and PoI information compiled from a large set of measurement data, as this increases the quality of information. On the other hand, they do not want to provide measurement data themselves, as this decreases their battery life (and also privacy). Therefore, this tussle is an instantiation of the common dilemma, where the benevolent act of an individual benefits the society but not the individual.

Thus, this tussle has to be resolved by developing a suited compensation mechanism for providing data. However, a monetary compensation is likely not scalable and requires additional information such as payment accounts.

4.5.2.5 Implications for symbIoTe

The adoption tussle discussed in Section 4.5.2.2 posed two questions that need to be answered in order to ensure that commercial IoT platform providers support symbIoTe. This support is mandatory for making the Smart Mobility and Ecological Routing use case a commercial success. In particular, it is necessary to provide incentive/compensation to commercial IoT platform providers to share data with symbIoTe. If such compensation can be found, the next question becomes how IoT platform providers can be prohibited from inventing data in order to receive higher compensation. Therefore, these questions have to be discussed and answered by the symbIoTe consortium. The guidance tussle, discussed in Section 4.5.2.3, will only be relevant, if these two questions are successfully answered. The battery tussle, discussed in Section 4.5.2.4, does not arise due to symbIoTe but is an instantiation of the common dilemma, where the benevolent act of an individual benefits the society but not the individual. As this tussle is independent of symbIoTe it is not considered a priority to be solved.

4.5.3 Value Network Analysis

The initial VNA version of the Value Network graphs is based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the use-case partners were conducted to finalize the VNA. In the following section a description of each VNA and its stakeholders can be found.

In this use-case following stakeholders are consider in the VNA: *symbIoTe, User, Wearable AQ IoT-Platform Provider, Stationary AQ Platform, Algorithm-Provider, Mobility Backend Provider, POI Provider, Government, Municipal/local Authorities, Data Owner, Sensor Provider,* and *Collective Mobility & local business*. In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 12.

The interaction between the stakeholders described in Table 12 can be observed in Figure 31. The *Stationary AQ-Platform* and the *Algorithm Provider* are two entities of the same institution in this case, which takes the role of the *Service Provider*. The Austrian Institute of Technology (AIT) is maintaining the *Stationary AQ-Platform* and are hosting and maintaining the symbIoTe platform as well as the code. The *Stationary AQ-Platform* provides air quality data of the existing network of air quality measuring stations across cities to *symbIoTe*. The *Stationary AQ-Platform* in return for payment receives sensors from the *Sensor Provider*, which are required for gathering the air quality data. The *Service Provider* as a whole has various interactions with other stakeholders. For once, the *Government* funds the AIT in return for data and knowledge on the air quality of its cities and the country in general. Further it handles the financial aspects for the symbIoTe platform. Therefore, it pays for the routing services provided by the *Mobility Backend Provider* to symbIoTe, as well as it pays for the air quality data provided to symbIoTe by the *Wearable AQ Platform*.

Table 12: VNA stakeholder description for UC Smart Mobility and Ecological Routing

Stakeholder	Description
symbIoTe	The intermediary platform to connect different data providers and data user with each other.

User	Is an end-user, which uses an symbIote enabled application or a website.
Wearable AQ IoT-Platform Provider	Company or institute gathering Air-Quality data via their mobile air quality sensors.
Stationary AQ Platform	Company or institute gathering Air-Quality data via their stationary air quality data. Often facilitated with governmental institutions.
Algorithm-Provider	Company or institute maintaining and hosting the symbIoTe platform.
Sensor Platform	Company producing air quality sensors.
Mobility Backend Provider	Company specialized in routing algorithms.
POI Provider	Open source platform providing data about point of interest in the city.
Government	Financing involved universities and research institutes.
Municipal/local Authorities	Commissioning local air quality data surveillance.
Data Owner	Person gathering air quality data with a mobile air quality sensor.
Collective Mobility & local business	Business and mobility provider including the smart mobility features into their application and webpage.

In return, AIT gets revenue by the *Collective Mobility & local business*, which are using the services and data provided through symbIoTe. These services and data include the air quality, ecological routing, PoIs, city air quality ratings, and any symbIoTe-enabled service developed in the future. This is often used as a complementary service for an already existing business e.g. ecological routing for a bike rental service. Thus, the *Collective Mobility & local business* is generating revenue in return for providing their core business services to its *Users*. The *Point-of-Interest Provider* is an open source service, which provides the point of interests for each city. In return they get an increase in their user base, which contribute with feedback to their platform and increase the quality of data they provide. The *Wearable AQ Platform* receives air quality sensors from the *Sensor Provider* in return for financial gratification. The *Wearable AQ Platform* is gathering its data by *Data Owners*, which use the wearable sensors. The *Data Owners* grant the platform to use their data and in return they get compensation. The compensation could be of financial nature or some other sort the *Data Owner* agrees on (i.e. vouchers or other goods). The *Wearable AQ Platform* is contracted by the *Municipal and local Authorities* for increasing the quality of air quality data gathering. The *Wearable AQ Platform* receives a form of license fee or maintenance fee for maintaining the platform and gathering the data. The *Municipal and local Authorities* get an instrument for better air quality monitoring and the life quality of its citizens get raised by providing it to them. This influences health of its population and increases the attractiveness of the city in the long term.

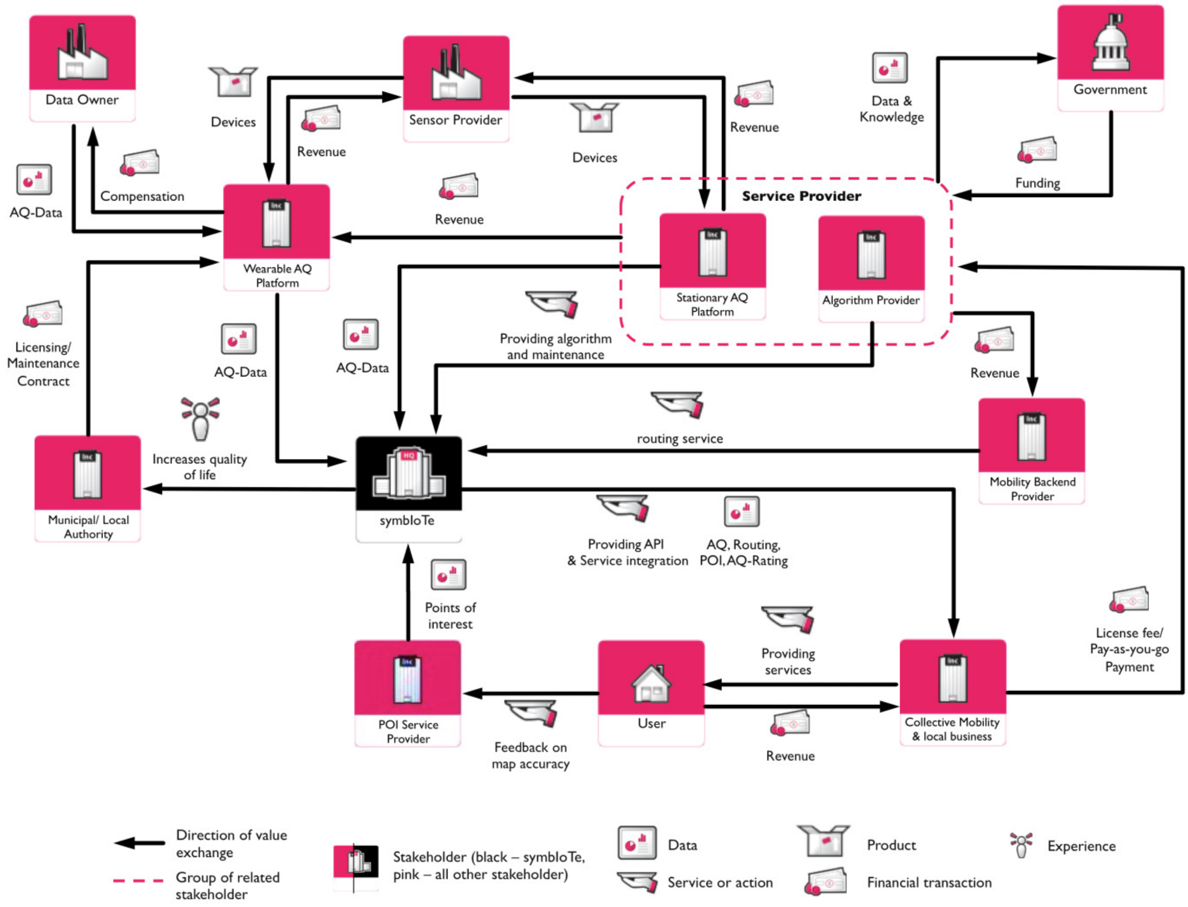

Figure 32: VNA Smart Mobility and Ecological Routing (represented according to symbIoTe prototypical demonstrations) [47].

4.6 Use-case 5: Smart Yachting

This section analysis the Smart Yachting use-case by presenting a CANVAS analysis in Section 4.6.1, applying tussle analysis in Section 4.6.2, and finally conducting a value network analysis in Section 4.6.3.

4.6.1 CANVAS Use-case Owner View

In Deliverable D1.3 [15] the initial version of the CANVAS for the use-case Smart Yachting was presented. The CANVAS building blocks were filled with input available end of 2016. Within the last 1.5 years some changes in the use-case have occurred, so that a new iteration of CANVAS was necessary to illustrate the current state. This status is based on the input provided by use-case owners and contributors, as well as on available more detailed description of use-cases and their intended show-cases as described in Deliverable D5.2 [35].

The involved partners decided as justified in Deliverable D5.2 [35] that the use-case Smart Yachting will cover two show-cases representing essential processes within a harbor, namely (1) Smart Mooring and (2) Automated Supply Chain. Only one CANVAS was developed summarizes the two showcases in the same scheme, because Smart Yachting is a single use case and a single business service. The two processes have the same key items (e.g., activities, resources, partnerships, costumers) and the same cost / benefit structure.

Show-case (1) – Smart Mooring - aims on automating the mooring procedure of the port, in itself a quite bureaucratic and tedious process, since Marinas operate in strongly regulated contexts. For the use case, the workflow logic is provided by a Navigo application called Portnet[50]. Here a particular phase of the Mooring process is intercepted and starts when the yacht is approaching – at a distance – the destination port and ends when it finally berths into one of the piers. When approaching the port, the yacht – as a symbIoTe's Smart Device– is detected by a component of the symbIoTe software infrastructure, namely the Smart Space's (SSP) Innkeeper, which associates the SDEV to the SSP and accordingly updates its properties in the symbIoTe Core. The use of both LoRaWAN and WiFi connections between the yacht and the port has been considered, the former to recognize when the yacht is near the port, but still at a distance, and the latter to allow the actual access to the yacht's resources by the Mooring Management application.

Show-case (2) – Automated supply chain - aims on automated identification of needs for goods and services on board of the yacht, so that automated requests for offers can be issued on the Marketplace platform of the port, provided in the trial by another application of the Navigo infrastructure, called Centrale Acquisti[51]. It assumes that the yacht is berthed at the port, and therefore steadily connected – through WiFi – to the port's SSP. While the yacht is berthed in the "smart" port, the yachtsman connects to the Centrale Acquisti Supply Chain application through a common web browser. He/she gives the authorization to Centrale Acquisti to connect through symbIoTe to the machine data of the boat, that automatically provides indication about what is needed on board, whether of maintenance or resupply nature. Needs are expressed by identifying the categories of the possible suppliers that might fulfill them by using the schema.org ontology[52] (e.g., the schema:Electrician class is used when maintenance on the electric systems of the yacht is needed).

Figure 33 shows the resulting CANVAS for the use-case assuming the following color scheme: Purple entries are issues related to citizens, green entries are issues related to developers, and yellow entries indicate general issues. It is obvious that key partnerships such as port authority and marinas, yachting service/facility providers, and yacht shipyards are also included in the envisioned customer segments as they are always involved. In customer segments software developers for ports, application (app) developers, and yachtsmen themselves are included. Key activities identified are promotion of new

[50] http://www.navigotoscana.it/navigo-partecipa-al-progetto-ue-symbiote-nel-programma-horizon-2020/ (May 18, 2018)

[51] http://www.navigotoscana.it/navigo-partecipa-al-progetto-ue-symbiote-nel-programma-horizon-2020/ (May 18, 2018)

[52] "schema.org is a collaborative, community activity with a mission to create, maintain, and promote schemas for structured data on the Internet, on web pages, in email messages, and beyond. Schema.org vocabulary can be used with many different encodings, including RDFa, Microdata and JSON-LD. These vocabularies cover entities, relationships between entities and actions, and can easily be extended through a well-documented extension model. Over 10 million sites use Schema.org to markup their web pages and email messages. Many applications from Google, Microsoft, Pinterest, Yandex and others already use these vocabularies to power rich, extensible experiences." (https: http://schema.org/, last visit May 12, 2018)

services, partner engagement, new service development opportunities for NavigoDigitale[53], strategic management and sales of new services. In order to perform the key activities key resources are essential, such as IoT platforms, interoperability layer, and NavigoDigitale, as well as symbIoTe L1 enablers, symbIoTe L4 smart spaces and roaming devices. The envisioned value proposition is manifold including among others interoperability with IoT platforms and third party service, automatic acquisition of boat data by port authority, quality and smart services for yachtsmen, improvement of logistics and tourism in landing coasts, and cloud based solution. In order to promote the developed solution different channels are used like B2C, direct sales, demonstration on events, online subscription, social networks, and website. Important customer relationships for this use-case are the yachting community, ports/marinas, partnership establishment, and connection to development communities. In order to meet the costs for business/software development, marketing, human resources, maintenance, and technical infrastructure different revenue streams come into focus. Those are service subscription, advertising, premium access packages, service activation and solution sales.

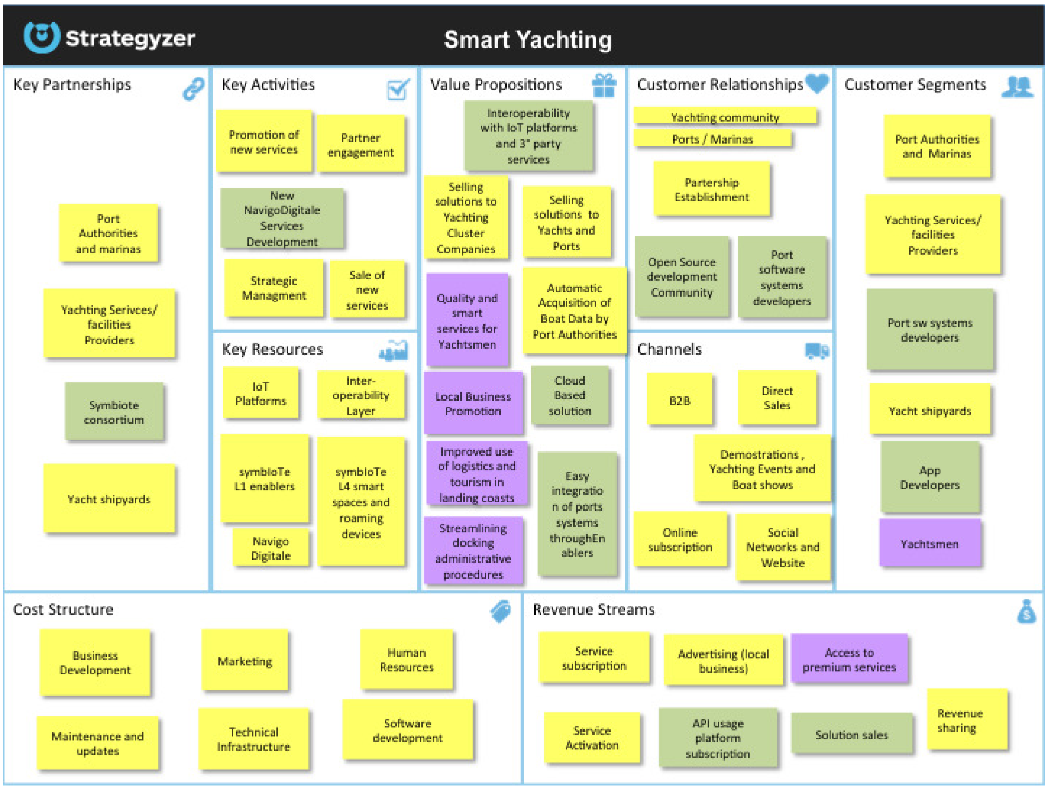

Figure 33: CANVAS for UC “Smart Yachting”

4.6.2 Tussle Analysis

This use case considers the mooring of yachts in a harbor and automates existing interactions in this scenario, such as the exchange of mooring documents or Wi-Fi passwords. Since the automated interactions are basic, no new tussles are created. The interactions are discussed in Section 4.6.2.2 and 4.6.2.3 to show that their automation

[53] http://www.navigotoscana.it/porti-turistici-del-futuro-grazie-alla-piattaforma-marina-iot/ (last visit May 18, 2018)

does not create new tussles. However, several tussles already exist without symbIoTe and evolve, for example, around data retention, secure data exchange, DDoS attacks, and request prioritization. As these tussles are out of symbIoTe's scope, they are not discussed here. Section 4.6.2.4 highlights next steps to be undertaken by the symbIoTe consortium. Next, stakeholders relevant for the discussions are introduced.

4.6.2.1 Stakeholders

The stakeholders that are relevant for the subsequent discussion are the harbor manager and the ship owner. Both stakeholders are an umbrella for different entities. For example, the ship owner comprises all entities on the ship, such as the captain, skipper, and/or sailor in charge. The interest of both stakeholders is to have a time efficient communication process with one another and to optimize cost/revenue when trading with one another. The stakeholders are summarized in Table 13.

Table 13: Stakeholders and their interests of the Smart Yachting use case

Stakeholder	Interest
Harbor manager	Time efficient communication process and optimized cost/revenue when trading with one another
Ship owner	

4.6.2.2 Mooring Document Exchange

symbIoTe aims to automate the exchange of mooring documents between a yacht and the harbor it approaches. When the information exchange between the harbor and yacht is automated via symbIoTe, it still will be conducted via the same communication channel. The only difference is that now no human-to-human communication is necessary as it is replaced by a machine-to-machine communication. This significantly reduces the effort to achieve the same result (the exchange of documents and mooring permission) and, therefore, is in the interest of harbor manager as well as ship owner. If the communication channel was secure before the introduction of symbIoTe, no new problems will be introduced by deploying symbIoTe. If the communication channel was not secure, security already had been an issue, before symbIoTe was introduced. Therefore, no security issues are introduced by symbIoTe.

4.6.2.3 Spare Part Comparison

symbIoTe aims to partially automate the purchasing of spare parts required by the ship. In particular, the compilation of parts that qualify to be purchased will be automated. This is done by automatically determining a list of items the yacht needs and comparing it to a list of items the harbor offers. The intersection of these two lists (or a select few available items matching a required item) is presented to the yacht owner, who selects the items to be purchased. As the ship is under the control of the ship owner, it can be assumed that it will present the ship owner with a list of items that allows him to make the most advantageous purchases. Therefore, as the ship owner still makes the final purchase decision, the ship owner has no disadvantage compared to when the process is conducted manually, i.e., without the symbIoTe solution. Also the harbor manager has no disadvantage, as he simply provides a list with his offerings and it does not make a difference for him, if this list is pre-processed by an algorithm.

4.6.2.4 Implications for symbIoTe

The Smart Yachting use case offers clear advantages for all involved stakeholders. However, adopting new software or hardware always implies additional costs. Therefore, stakeholders in charge of the yacht as well as of the harbor have to be convinced of the benefits symbIoTe offers to the mooring process. These benefits are an eased mooring process and eased purchase of spare parts. Therefore, the next steps for the symbIoTe consortium are to compile these arguments into convincing demonstrations and develop an action plan to approach relevant stakeholders with this presentation material.

4.6.3 Value Network Analysis

This use-case consists of two showcases (1) Smart Mooring, and (2) Smart Supply Chain. For each of the showcases an individual VNA was conducted. The initial VNA versions of the VNA graphs are based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the use-case partners were conducted to finalize the VNA's. In the following section a description of each VNA and its stakeholders can be found.

4.6.3.1 VNA for Show-case on Smart Mooring

The initial VNA version of the VNA graphs is based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the use-case partners were conducted to finalize the VNA. In the following section a description of each VNA and its stakeholders can be found.

In the use-case Smart Yachting, showcase (1) Smart Mooring following stakeholders are consider in the VNA: *Yacht/Yachtsman, Port Personnel, symbIoTe, Yacht IoT-Platform, Port IoT-Platform, Port Authority Operator, Port Authority/Management, Mooring Workflow Platform,* and *Sensor/Beacon Provider.* In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 14.

The interaction between the stakeholders described in Table 14 can be observed in Figure 34. *SymbIoTe* connects the *Port IoT-Platform*, the *Yacht IoT-Platform* and the *Mooring Workflow Platform* and enables the Platforms to share data between each other. This allows to automate the whole mooring workflow and reduce the work for *Yachtsman* as wall as *Port Authority Operator* and *Port Personnel*. The *Port IoT-Platform* and *symbIoTe* operators get a maintenance fee and contract fee from the *Port Authority and Management* for keeping the platform up and running. The platform sends sensor data from around the port to symbIoTe as well the *Port IoT-Platform* operator maintains symbIoTe. The *Mooring Workflow Platform* receives sensor data from the port sensors as well as from the yacht sensors via symbIoTe and sends notifications via symbIoTe to the Yacht IoT-Platform. The *Sensor and Beacon Suppliers* provide devices to the *Port IoT-Platform* as well as to the *Yacht IoT-Platform*. In return they receive revenue in case of the *Port IoT-Platform* from the platform operator and in case of the *Yacht IoT-Platform* from the *Yachtsman.* The *Yacht IoT-Platform* forwards notifications sent from the *Mooring Workflow Platform* to the *Yacht and Yachtsman.* Furthermore, the *Yacht* shares its sensor data and location with the *Yacht IoT-Platform*. The *Yacht and Yachtsman* initiates the whole mooring process with a service request i.e. booking a mooring spot by contacting the *Port Personnel*. In a next step, the *Port Personnel* is initiating the mooring workflow in the *Mooring Workflow Platform*. In return, the *Mooring Workflow Platform alerts the Port Personnel*. This could be an automatic alert generated by the platform itself or originating from the *Port Authority Operator*, which sends alerts and information to the *Mooring Workflow Platform*. The *Port Authority Operator* handles all requests and accesses for data and mooring permissions sent via the *Mooring Workflow Platform*. The Port Authority

Operator is briefing the *Yacht and Yachtsman* and conducts the payment of the *Yachtsman* and forwards the collected payment to the *Port Authority and Management*.

The benefit of including *symbIoTe* is the possibility to connect various *Port IoT-Platforms* with various *Yacht IoT-Platforms* and allows simplifying and automating the mooring process. This reduces the paperwork on both *Yachtsman* as well as *Port Authority Operator* side and speeds up the process.

Table 14: VNA stakeholder description for UC Smart Yachting - Smart Mooring

Stakeholder	Description
symbIoTe	The intermediary platform to connect the different platforms from port and yacht.
Yacht/Yachtsman	The yacht or captain of the yacht trying to moor in the port.
Port Personnel	Operates the whole infrastructure in the port and providing the services to the yacht/yachtsmen.
Yacht IoT-Platform	The yachts own IoT-Platform connecting all sensors and the board computer.
Port IoT-Platform	The ports IoT-Platform connecting all sensors in and around the port, providing its data to the port personnel and other applications.
Port Authority Operator	Handles all administrative and official paperwork regarding the yacht registration etc.
Port Authority/Management	Managing the port and handling all financial aspects related to the port.
Mooring Workflow Platform	Platform, which automatically updates the yachts status and informs the affected parties in each step.
Sensor/Beacon Supplier	Provides the necessary sensors and beacons to the platforms. This is just illustrative, there are numerous different supplier in real world.

4.6.3.2 VNA for Show-case on Smart Supply Chain

The initial VNA version of the VNA graphs is based on the descriptions in deliverable D1.3 and D5.2. Further discussions with the use-case partners were conducted to finalize the VNA. In the following section a description of each VNA and its stakeholders can be found.

In the use-case Smart Yachting, showcase (2) Smart Supply Chain following stakeholders are consider in the VNA: *Yacht/Yachtsman, symbIoTe, Yacht IoT-Platform, Port IoT-Platform, Sensor/Beacon Provider, Service Provider,* and *Port Authority/Management.* In order to understand the role of each stakeholder in the context of this showcase a short description is provided in Table 15.

The interaction between the stakeholders described in Table 15 can be observed in Figure 35. SymbIoTe is hosted and maintained by the *Port IoT-Platform* and it connects the *Port IoT-Platform* and the *Yacht IoT-Platform*. It shares the sensor data of the *Yacht* with the *Port IoT-Platform* and the list of service suppliers and shares offers compiled to fit the needs of the *Yacht and Yachtsman* with the *Yachtsman*. The *Service Provider* provides the services or goods requested by the *Yachtsman* in return for a payment agreed on by the two parties. The *Service Provider* gets access to offer his services and products on the *Port IoT-Platform* by paying a license fee to the *Port Authority and Management*, which is contracting the *Port IoT-Platform* operator. The *Sensor and Beacon*

Supplier takes in this showcase the same role as in the first showcase (1) Smart Mooring by supplying sensors to the *Port* and *Yacht IoT-Platform*.

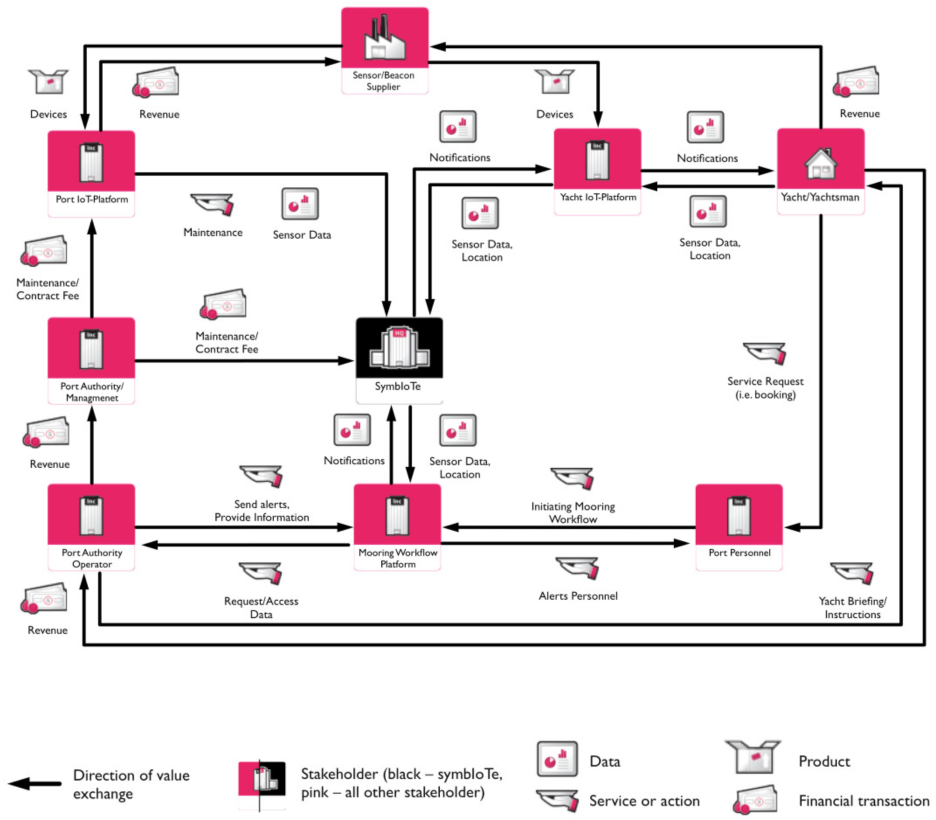

Figure 34: VNA UC Smart Yachting, Show-case (1) Smart Mooring [47].

Table 15: VNA stakeholder description for UC Smart Yachting - Smart Supply Chain

Stakeholder	Description
symbIoTe	The intermediary platform to connect the different platforms from port and yacht.
Yacht/Yachtsman	The yacht or captain of the yacht trying to request a service at the port.
Yacht IoT-Platform	The yachts own IoT-Platform connecting all sensors and the board computer.
Port IoT-Platform	The ports IoT-Platform connecting all sensors in and around the port, providing its data to the port personnel and other applications.
Service Provider	Provides all services to the yacht and the yachtsman. The services can either be of maintaining nature or consumable nature.
Port Authority/Management	Managing the port and handling all financial aspects related to the port.
Sensor/Beacon Supplier	Provides the necessary sensors and beacons to the platforms. This supplier is just illustrative, in real world there are numerous different supplier.

The benefit of including *symbIoTe* is the possibility to connect various *Port IoT-Platforms* with various *Yacht IoT-Platforms* and offer additional services to *Yacht and Yachtsman* in an easy way. Furthermore, it creates a new revenue stream for the *Port Authority and Management* with the license fees of the *Service Providers*.

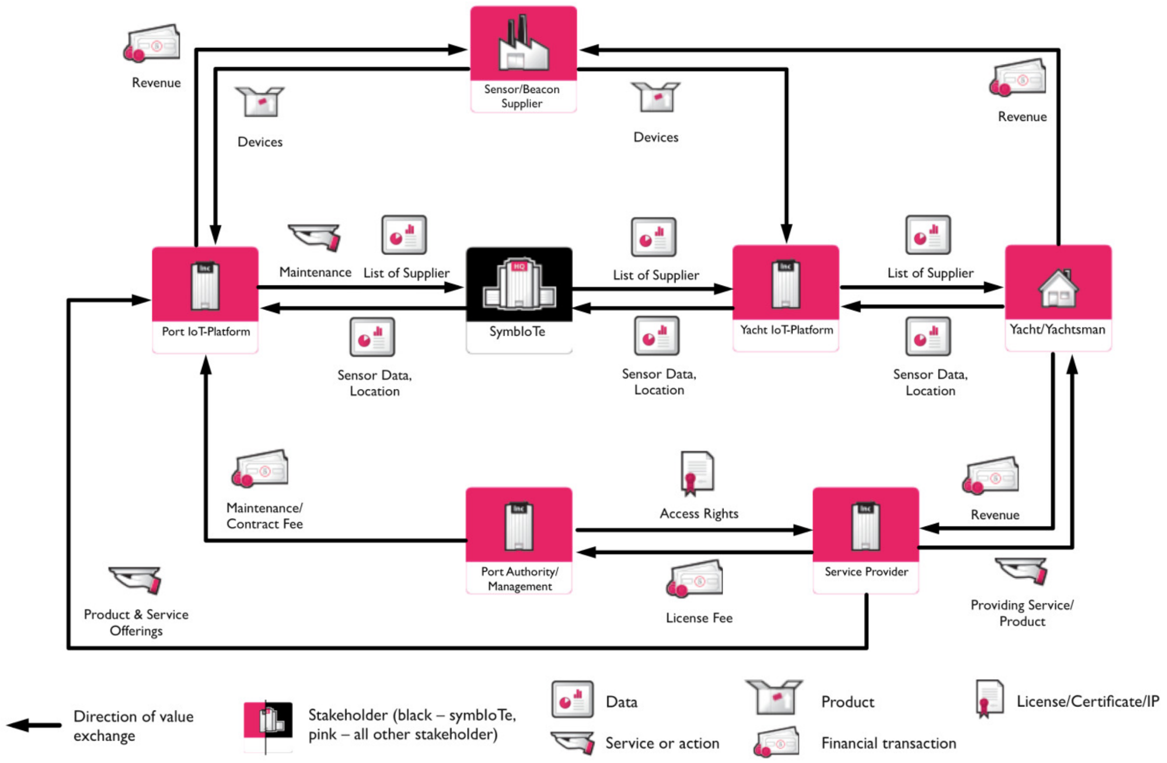

Figure 35: VNA UC Smart Yachting, Show-case (2) Smart Supply Chain [47].

5 symbIoTe's Business Model and Sustainability Recommendation

The findings of Section 4 to each use-case consisting of the business CANVAS, the Tussle analysis and the VNA allow the definition of a business model recommendation. The goal of this business model recommendation is not only to address the best way to operate the symbIoTe platform in each use-case in a monetary perspective. Furthermore, it focuses on a sustainable setup for operating the symbIoTe after project end. For this reason short-term actions and intrinsic motivations of key stakeholders get addressed to keep the stakeholders engaged in the network not only short-term, but rather in a sustainable long-term arrangement. Key stakeholders are stakeholders, which are critical for running the business model and are a subset of stakeholders from the VNA. Using the approach of Terrenghi, Schwarz and Legner [45] motivations are identified and then categorized in short term and long term, as well as economical, social and ecological motivations. A description of mentioned process is provided in the Appendix 9.2. By categorizing the motivations it becomes more obvious to see the nature of the motivations and addressing stakeholders interests in the platform easier. The motivations of the stakeholders can be leveraged to develop specific features in future and keep the stakeholders engaged in the long term in each use-case.

While the business models get addressed in this section, the bundling of the offers and specifications of the single pricings are not subject of this section and will be further explored in the WP7.

5.1 Use-case Specific Recommendations

In the following subsections the business model recommendation and identified items for sustainability are presented. The sustainability items can be divided into short and long term items. Appendix 9.2 includes the respective sustainability graphs.

5.1.1 Use-case 1: Smart Residence

The business model advisable for all show-cases would be to run symbIoTe as a company, which is hosting and maintaining the system. The company is preferably one of the involved use-case partners or could optionally be an independent startup. The reward the company receives is a combination of a license fee and a pay-by-use or number-of-registered-devices fee for the service it provides to the Home Automation Service Providers. The license fee grants permission to the network and the variable part of the fee should cover the run-time costs and maintenance.

A further possibility for the (3) Active and Assisted Living show-case is to apply for insurance coverage or subsidies for connecting the Smart Mirror to the Tele-health-Platform.

The goal in the future would be to create a symbIoTe-enabled label for IoT-Platform in the Smart Residence sector for platforms using symbIoTe. According to the Boston Consulting Group [48], there is going to be a war between IoT-Platforms. This results in big competition between small platforms and big platforms, a competition with unfair advantage for the big platforms unless the small platforms federate. For that reason, a strategy toward sustainability would be to address companies or startups with small IoT-Platforms to join the symbIoTe and enable their platforms. Once a community of small IoT-Platform providers has formed, companies with bigger IoT-Platform could get targeted.

In regard of a sustainable devolvement in the long term, motivations for participating the platform of each key stakeholder have to be identified. Due to the similarity of the show-case (1) Healthy Indoor Air and (2) Smart Residence both show-cases are covered in the section below. The identified key stakeholders in the show-cases that are key drivers in the whole business model are the Resident, the Home Automation Service Provider, Government, and Weather Stations/Public Administration (cf. Table 2 for a stakeholder description). Each of the stakeholders has his own motivations to participate in the network, which can be found in Table 16. A visible representation in form of a graph for a better understanding can be found in the Appendix 9.2. The graph illustrates how the key stakeholders relate to each other and shows to the motivations addressing the Smart Residence (1) Healthy Indoor Air show-case.

Table 16: Smart Residence sustainability stakeholder motivation.

Stakeholder	Motivation
Resident	Better indoor air quality Health benefits Saving on heating and cooling (cost reduction) Increased comfort
Home Automation Service Provider	Increased innovation Increased sales Build reputation Increase loyalty Attracting new customers
Government	Map city needs Optimization of city planning in regards of air quality Better and healthier air condition for citizens
Weather station/ Public administration	Receive public funding Create knowledge

The motivations of the key stakeholders of the (1) Healthy Indoor Air and (2) Smart Residence show-cases are then categorised and presented in the Table 17.

While there are economic short-term effects like time increasing sales, attracting new customers, and receive public funding or social motivations like better indoor air quality, heath benefits, and increased comfort, which motivates the stakeholders to be in favour of the system in the immediate future. There are long-term motivations highlighting the greater goal stakeholders aim for. The short-term motivations are related to implications affecting the stakeholders on a daily basis. The long-term motivations on the other side have more far reaching goals. Economical once aim at saving on heating and cooling (cost reduction), increased innovation, increased sales, attracting new customers, and receive public funding. In the social category there is the better indoor air quality, health benefits, increased comfort, build reputation, increase loyalty, create knowledge, optimization of city planning in regards of air quality, and better and healthier air condition for citizens. The motivations are focused at better quality of life, for the resident this is on the inside of his/her home and for the government it is independent of location since it affects the citizens health in the long run. At last the ecological categories with mapping the city's needs and better and healthier air condition for citizens, relating both an optimization of city planning in regards of air quality. The granularity of the air quality data increases by including the air quality of smart residences, which allows to better analyse the cause of air pollution and plan better-suited counter measures.

In order to keep the key stakeholder motivated after project end, first the short-term motivations should be met by functions of symbIoTe. After short-term motivations are met, a prioritisation of long-term motivations, which are not already fulfilled, should follow. The most important motivations should then get translated in features for future releases. This allows keeping the stakeholders interested and involved in the platform.

Table 17: Smart Residence sustainability stakeholder motivation categorised.

	Short-term	**Long-term**
Economical	Increased sales Attracting new customers Receive public funding	Saving on heating and cooling (cost reduction) Increased innovation Increased sales Attracting new customers Receive public funding
Social	Better indoor air quality Health benefits Increased comfort	Better indoor air quality Health benefits Increased comfort Build reputation Increase loyalty Create knowledge Optimization of city planning in regards of air quality Better and healthier air condition for citizens
Ecological		Map city needs Optimization of city planning in regards of air quality Better and healthier air condition for citizens

5.1.2 Use-case 2: EduCampus

First of all, it would be advisable to focus on the (1) Campus Federation show-case since its success is critical to the whole use-case. The (2) connecting third-party services to the campus platform show-case is a complementary and optional add-on for future developments.

The two business models fitting this use case are the licensing model and the open source model. Which one will be chosen depends highly on if one university takes the lead. Both models will be explored briefly since this decision is not taken.

The recommended model with a business for profit would be a licensing approach. One of the two universities already involved in the project hosts and maintenances symbIoTe or develops the platform further in the future. In return it receives a license fee from each university that join the network as well as from the 3rd-Party Service Provider for accessing the platform. This model would be close to a commercial business model, which would be an incentive for the operating university to host it depending on how it’s priced. Beneficial for the system would be that there is just one organization and one team responsible for symbIoTe and they know the needs of its campus users and other stakeholders from university. They could as well steer the development of symbIoTe for a long-term satisfaction of all stakeholders.

If no university wants to take the responsibility an open source strategy would be possible as well. Each university joining the network would be responsible for hosting their own symbIoTe setup and keeping it up to date. A community of the partner university would be responsible for future platform developments. A committee with members of each contributing partner university should be formed to make decisions on the systems development. 3rd-Party Service Providers could register and offer their services for free or for an access fee directly to the university on the platform. The costs for operating the platform on their infrastructure would have to be covered by each university itself.

In order to join the network federated universities have to accept a service level agreement (SLA) in order to participate in the network, independent of which business model is in place. Policy, Responsibilities, Security Issues as well as financial matters are defined in the SLA. In case of the license fee universities have to pay individual fees by either number of user's, monthly subscription or pay-by-usage and should cover the maintenance costs. Pricing and bundling options will be explored further in detail in WP7. If it is an open source model required non-monetary contribution to the network and community have to be defined in the agreement as well.

In order to keep symbIoTe up and running after the end of the project an agreement with the universities already involved in this use-case should be made, which encourages them to use and maintain symbIoTe further. In a next step, the other universities involved in the symbIoTe project should get inquired to implement the basic functions of the first show-case (1) Campus Federation. This would build the basics of a community and encourage other universities not part of the project to join the symbIoTe - EduCampus platform.

symbIoTe as binding link between individual platforms and users is only of relevance if there are partner universities and service providers providing access and services to its campus users for this reason it is critical to build a solid foundation of key partner universities from the beginning.

A further possibility could be to contact the EduRoam[54] committee funded by the GÉANT Project, which have already build an international community of universities around the globe for unifying Internet access at the campus.

With regards to the development of the platform in a sustainable way in the long-term, motivations of each key stakeholder have to be identified and be met in the future. The identified key stakeholders in the EduCampus use case that are key drivers in the whole business model are the Campus User, Administration of University, University (Management), and 3rd-Party Service Provider. Each of the stakeholders has his own motivations, which can be found in Table 18. A visible representation for a better understanding on how we derived to the motivations addressing the campus federation can be found in the Appendix 9.2.

The motivations of the key stakeholders of the campus federation showcase are then categorised and presented in the Table 19.

While there are short-term effects like time saving and better fitting location motivates the stakeholders to be in favour of the system in the immediate future, the long-term motivations highlight the greater goal stakeholders aim for. Most of the short-term

[54] https://www.eduroam.org/ (last visit May 31, 2018)

motivations are related to time saving, faster access, better fitting location or reduced paperwork, which would simplify the working routine on a daily basis. The long-term motivations on the other side have more far reaching goals.

Table 18: EduCampus sustainability stakeholder motivation.

Stakeholder	Motivation
Campus User	Time saving Better fitting location Immediate access to administration services Immediate access to 3rd-party services
Administration of University	Time saving Efficient room usage/occupation Reduced paperwork
University (Management)	Reducing costs Increase transparency for funding opportunities Increase attractiveness of work environment Reduced effort and cost for access Increase room planning efficiency Improve image
3rd-Party Service Provider	Direct access to customer Easier way of service offering Reduced paperwork Easier way of offering new services

Table 19: EduCampus sustainability stakeholder motivation categorised.

	Short-term	Long-term
Economical	Time saving Better fitting location Direct access to customer Easier way of service offering	Efficient room usage/occupation Reducing costs Increase transparency for funding opportunities Easier way of offering new services Improve image
Social	Time saving Better fitting location Immediate access to administration services Immediate access to 3rd-party services	Increase attractiveness of work environment Reduced effort and cost for access Improve image
Ecological	Better fitting location Reduced paperwork	Increase room planning efficiency

Economical ones aim at better room usage, cost reduction, getting better insights on which room size and type is more frequent requested, improving the image or reduce the effort to advertise new services. In the social category there is the increased attractiveness of work environment through its added services, improving the image and the reduced administrative effort and cost for access. This triggers better accessibility for its users lowers the barrier for collaboration and exchange across partner universities and improves the knowledge transfer. This is beneficiary for the university in terms of knowledge gain itself as well as the impact on university ranking factors such as international faculty/student ratio[55], which have a measurable value to the university. Improving the image has economical as well as social aspects since an improved image attracts more students, which as a result will pay more tuition fee. At last the ecological category with an increased room planning efficiency, which would lead to less and better fitting rooms and therefore, less buildings needed.

In order to keep the key stakeholder motivated after project end first the short-term motivations should be met by functions of symbIoTe. After short-term motivations are met a prioritisation of long-term motivations, which are not already fulfilled should follow. The most important motivations should then get translated in features for future releases. This allows keeping the stakeholders interested and involved in the platform.

5.1.3 Use-case 3: Smart Stadium

The three showcases of the Smart Stadium Use case, (1) Visitor Application, (2) Retailer Application, (3) Promowall are built each one on top of the previous one. Thus, the same business model is envisaged for the three of them. There are, however, two options for managing symbIoTe, one is having the platform managed by symbIoTe consortium and thus, the Stadium owner must pay the maintenance fee; and the second one is managing its own installation and thus just pay a license fee to the consortium.

In the first case, the only business interaction would be between symbIoTe and the Smart Stadium Providers, which would pay a fee for using symbIoTe and getting added value services (i.e. hosting and maintenance). In the other case, the Smart Stadium Provider would host symbIoTe himself and would generate revenue by operating the Smart Stadium as well as symbIoTe, paying a license fee.

Independent of who is operating symbIoTe the (3) Promowall show-case has the possibility of an additional revenue stream. A fee for advertising on the Promowall could be sold to the Stadium Manager, which is contracting the retailers for advertising in the stadium. This would maximize the revenue further.

In order to have a real-value use case, the usage of symbIoTe is mandatory as it allows the interaction of different platforms in a simple manner, and allows the replication within different stadiums or sport areas. For this reason, a third party acting as a symbIoTe provider is needed. It can be each Stadium owner, who manages his own installation, or more likely the symbIoTe consortium who offers the service (symbIoTe as a Service) or an external company (license-based). Taking into account the complexity of symbIoTe, the most suitable option is that symbIoTe consortium assures the availability of results and supporting team once the project has ended. This would ensure that the symbIoTe technology is used in the context of Smart Stadium and other supplier of IoT-Platform solutions would get in touch with symbIoTe over time and adopts symbIoTe as a standard.

In order to have a long-term sustainable ecosystem, motivations for participating in the platform of each key stakeholder have to be identified. Due to the similarity of the show-case (1) Visitor Application and (2) Retailer Application both show-cases are covered in the section below. The identified key stakeholders in the show-cases that are key drivers in the whole business model are the Visitor, the Retailer, and the Stadium Manager (see

[55] https://www.topuniversities.com/qs-world-university-rankings/methodology (last visit May 31, 2018)

Table 2 for a stakeholder description). Each of the stakeholders has his own motivations to participate in the network. A visible representation in form of a graph for a better understanding on how we derived to the motivations addressing the Smart Stadium (1) Visitor Application show-case can be found in the Appendix.

Table 20: Smart Stadium stakeholders‘ motivation.

Stakeholder	Motivation
Visitor	Reducing hassle in getting services and goods Avoid queuing Easy moving around
Retailer	Avoid peak rush Increase revenue/profit Increase efficiency Lower cost (staff) Offer more valuable services
Stadium Manager	Reduce overcrowding (crowd management) Better utilization of retailer space Improve venue image Better information on visitors behaviour /demographic (insights) Increased revenue to from more added-value services Attract more visitors

The motivations of the key stakeholders of the (1) Visitor Application and (2) Retailer Application show-cases are then categorised and presented in the Table 21.

While there are economic short-term effects like easy moving around, lower cost (staff), increase revenue/profit, and increased revenue to from more added-value services or social motivations like reducing hassle in getting services and goods, avoid queuing, avoid peak rush, reduce overcrowding (crowd management), and better information on visitors behaviour /demographic (insights), which motivates the stakeholders to be in favour of the system in the immediate future. There are long-term motivations highlighting the greater goal stakeholders aim for. The short-term motivations are related to implications affecting the stakeholders on a daily basis. The long-term motivations on the other side have more far reaching goals. Economical once aim at better utilization of retailer space, improve venue image, and increase efficiency. In the social category there is offer more valuable services, improve venue image, and attract more visitors. The motivations are focused at developing a better visitor experience at the stadium over time. At last there is the ecological category with increasing efficiency, which would result in a more careful usage of the given resources.

In order to keep the key stakeholder motivated after project end first the short-term motivations should be met by functions of symbIoTe. After short-term motivations are met a prioritisation of long-term motivations, which are not already fulfilled should follow. The most important motivations should then get translated in features for future releases. This allows keeping the stakeholders interested and involved in the platform.

Table 21: Smart Stadium stakeholder motivation categorised.

	Short-term	Long-term
Economical	Easy moving around Lower cost (staff) Increase revenue/profit Increased revenue to from more added-value services	Better utilization of retailer space Improve venue image Increase efficiency
Social	Reducing hassle in getting services and goods Avoid queuing Avoid peak rush Reduce overcrowding (crowd management) Better information on visitors behaviour /demographic (insights)	Offer more valuable services Improve venue image Attract more visitors
Ecological		Increase efficiency

5.1.4 Use-case 4: Smart Mobility and Ecological Routing

The AIT, which is hosting the symbIoTe platform in this use-case has multiple possibilities to create revenue. The primary revenue stream is from collective mobility provider and local companies paying for using the ecological routing services provided by symbIoTe. Another revenue stream is advertisement space, which can be sold to customers buying the routing services or complete different customers. However, for authenticity reason it would be advisable to constrain advertisers to the ecological and sportive sector. The last revenue stream is from the government, which provides additional funding to AIT for increased insights and data on air quality.

Beyond this further revenue streams may included when the use case is transferred to adjacent cases with similar technological or service needs.

For the first phase after the end of the project AIT volunteered to look into the possibility of operating symbIoTe in this context. In order to keep symbIoTe attractive for AIT it is important to attract business and collective mobility providers to adapt the ecological routing service and maybe into the option of setting up symbIoTe in new cities as well by partnering with local software companies. This would provide AIT as well the option to reduce their involvement in the future, if the project is not evolving according to expectations (negative case) or if the business case scales beyond the core interest of AIT (positive case).

In regard of a sustainable devolvement in the long term, motivations for participating the platform of each key stakeholder have to be identified. The identified key stakeholders in the Smart Mobility and Ecological Routing show-case, that are key drivers in the whole business model are the User, Government, Service Provider (Algorithm Provider and Stationary AQ-Platform Provider combined) and Wearable AQ Platform Provider (see Table 10 for a stakeholder description). Each of the stakeholders have their own motivation to participate in the network, which can be found in Table 22. A visible representation in form of a graph for a better understanding on how we derived to the motivations addressing the Smart Mobility and Ecological Routing use-case can be found in the Appendix 9.2.

Table 22: Smart Mobility sustainability stakeholder motivation.

Stakeholder	Motivation
User	Less polluted routes Increase health benefits Explore new routes
Collective Mobility & local business	Increase attractiveness of service Improve image Sell healthy products to users
Service Provider (Algorithm + Stationary AQ-Platform Provider)	Create knowledge for public funding Better air quality data that can be materialized on for adjacent cases (e.g., consulting businesses in real estate development)
Government/City Authority	Map city needs Improve health of citizens Better and healthier air condition for citizens Increase attractivity of city by motivating more users to switch to bicycles (e.g., reduction of cars, more humans on the street to interact with local businesses) Optimization of city planning in regards of air quality Realize synergies for city planning, e.g., reduction of the increasing demands for car traffic may reduce infrastructure investments
Wearable AQ-Platform Provider	Create knowledge for public funding Gather better air quality data in order to build a technologically superior offering for future projects and clients with specific needs Increase revenue, due to easier accessible sales channel

The motivations of the key stakeholders of the Smart Mobility and Ecological Routing use-case are then categorized and presented in the Table 23.

Table 23: Smart Mobility sustainability stakeholder motivation categorized.

	Short-term	Long-term
Economical	Create knowledge for public funding Better air quality data that can be materialized on for adjacent cases (e.g., consulting businesses in real estate development)	Create knowledge for public funding Increase attractiveness of service Improve image Gather better air quality data in order to build a technologically superior offering for future projects and clients with specific needs Realize synergies for city planning, e.g., reduction of the increasing demands for car traffic may reduce infrastructure investments
Social	Less polluted routes Explore new routes Sell healthy products to users	Improve health of citizens Better and healthier air condition for citizens Optimization of city planning in regards of air quality Increase attractivity of city by motivating more users to switch to bicycles (e.g., reduction of cars, more humans on the street to interact with local businesses
Ecological		Map city needs Optimization of city planning in regards of air quality Better and healthier air condition for citizens Increase attractivity of city by motivating more users to switch to bicycles (e.g., reduction of cars, more humans on the street to interact with local businesses)

While there are economic short-term effects like create knowledge for public funding or that can be materialized on for adjacent cases (e.g., consulting businesses in real estate development) and social motivations like less polluted routs, explore new routes, and sell healthy products to users, which motivates the stakeholders to be in favor of the system in the immediate future. There are long-term motivations highlighting the greater goal stakeholders aim for. The short-term motivations are related to implications affecting the stakeholders on a daily basis. The long-term motivations on the other side have more far reaching goals. Economical once aim as well at create knowledge for public funding in the long-term or improve the attractiveness and image of the local business. In the social category the motivations are improve health of citizens, better and healthier air condition for citizens, optimization of city planning in regards of air quality, and increase attractivity of city by motivating more users to switch to bicycles (e.g., reduction of cars, more humans on the street to interact with local businesses). The motivations are focused at better quality of life and health, for the user and citizen, which has a further positive effect on the cost of related health issues. At last the ecological category with mapping the city's needs and better and healthier air condition for citizens, relating both an optimization of city planning in regards of air quality and inefficient routing as well as increase attractivity of city by motivating more users to switch to bicycles (e.g., reduction of cars, more humans on the street to interact with local businesses). The granularity of the air quality data increases by including the mobile air quality sensors, which allows to better analyze the cause of air pollution and plan better-suited counter measures.

In order to keep the key stakeholder motivated after project end first the short-term motivations should be met by functions of symbIoTe. After short-term motivations are met a prioritization of long-term motivations, which are not already fulfilled should follow. The most important motivations should then get translated in features for future releases. This allows keeping the stakeholders interested and involved in the platform.

5.1.5 Use-case 5: Smart Yachting

The business model in the two show-cases (1) Smart Mooring and (2) Automated supply chain are not the same since different stakeholders are involved, but are complementing the revenue streams. In both show-cases the company behind the port IoT-Platform operates symbIoTe and receives a maintenance or contract fee for operating the platform. The fee's amount depends highly on the size of the port, number of integrated sensors or number of mooring processes. An additional revenue stream is added when considering (2) Automated supply chain show-case. Local business owners have to register with the Port Authority/Management and pay a subscription fee for joining the platform. Part of this subscription fee is adding to the contract fee between the port authority/management and the IoT-Platform operator.

In future developments other business models could be included as well i.e. fees for access to premium services or advertising options for local business.

In order to keep the Smart Yachting platform open after the project terminates, it is important to encourage the industry partners of this use-case to use the symbIoTe technology in the future. The status of the platform in the end of the project should reach a point, which allows the industry partner to use the technology as a steppingstone and leverage it for further developments. The first steps after project end should be to setup the system in further ports near by the already symbIoTe enabled port. This would create a need on side of the local yacht IoT-Platform operatorr to integrate into the ecosystem. It is important to start the distribution of the platform in one area or following high frequent used yachting routs in order to get the attention of the yachtsman and form the desire to have this setup in every port.

In regard of a sustainable devolvement in the long term, motivations for participating the platform of each key stakeholder have to be identified. The identified key stakeholders in the show-case (1) Smart Mooring, that are key drivers in the whole business model are the Yachtsman, the Port Authority Operator, the Port Authority Management, and the IoT-Platform Provider (see Tables 14 and 15 for a stakeholder description). Each of the stakeholders has his own motivations to participate in the network, which can be found in Table 24. A visible representation in form of a graph for a better understanding on how we derived to the motivations addressing the Smart Yachting (1) Smart Mooring show-case can be found in the Appendix 9.2.

Table 24: Smart Yachting sustainability stakeholder motivation.

Stakeholder	Motivation
Yachtsman	Reduce administration process time Reduce document work Reduce and control the time of mooring Increased yacht security
Port Authority Operator	Increase customer capacity Increase attractiveness of port Increase docks management control Time saving
Port Authority Management	Increase productivity Increase management control Increase port security Reduce paper storage
IoT-Platform Provider	Increase business Increase business data Increase number of services

The motivations of the key stakeholders of the (1) Smart Mooring show-case are then categorised and presented in the Table 25.

Table 25: Smart Yachting sustainability stakeholder motivation categorised.

	Short-term	Long-term
Economical	Increase docks management control Time saving Increase productivity Increase management control Increase business	Increase customer capacity Increase attractiveness of port Increase business data Increase number of services
Social	Increased yacht security Time saving	Reduce administration process time Reduce and control the time of mooring Increase attractiveness of port Increase port security
Ecological	Reduce document work Reduce paper storage	

While there are economic short-term effects like increased docks management control, time savings, increased productivity, increased management control, and increase business, social motivations like increased yacht security and time savings as well as ecological in reducing document work and paper storage. The short-term motivations are related to implications affecting the stakeholders on a daily basis and in the immediate future. There are long-term motivations highlighting the greater goal stakeholders aim for. These motivations have more far reaching goals, the economical once aim at increased customer capacity, increased attractiveness of port, increased business data, and increased number of services. In the social category there is reduce administration process time, reduce and control the time of mooring, increase attractiveness of port, and increase port security. The motivations in both categories are focused at creating a more efficient mooring process in terms of process time and smoother operations and better management of capacities. These improvements are not only affecting port related stakeholder, but increases the attractiveness of the port and adds value for the yachtsman as well.

In order to keep the key stakeholder motivated after project end first the short-term motivations should be met by functions of symbIoTe. After short-term motivations are met a prioritisation of long-term motivations, which are not already fulfilled should follow. The most important motivations should then get translated in features for future releases. This allows keeping the stakeholders interested and involved in the platform.

5.2 Global Applicable Recommendations

The realization of one business model for the symbIoTe solution would not only be a great challenge, but rather an almost impossible endeavor. Each use-case is not only using different technologies or enablers for interpreting the data of its IoT-Platforms, is as well situated in completely different industries and fields. Thus, it requires different knowledge in terms of technology and different insights in the markets as well. Consolidating this into on single business would require a big company already involved in each industry and versatile in the different technologies to take the lead. Since such companies tend to develop their own platforms and solution, another road would promise more success for a longlivity of the symbIoTe solution. It would be advisable to treat each use-case as a separate solution after the end of the project, encouraging involved project partners to develop and implement their use-case specific platform independent of each other with symbIoTe as an underlying framework.

Independent of the use-case, it is needless to mention that for IoT-Platforms and platforms in general the network effect is crucial. In network effect and platform strategy research platforms are often defined as multi-sided markets in which providers offer goods or services to the user on the other side [50, 51]. The theory suggests strategies for aggressively attracting such providers, which results in a rise in demand on user side and a demand on the provider side in return evolving into a network effect with a winner-take-all characteristic [52, 53]. Same applies for the symbIoTe enabled IoT-Platforms. The more symbIoTe enabled platforms there are, the more other platforms get attracted. Thus, it is critical to build a solid foundation of platforms already enabled, when starting the business. IoT-Platform providers could get recruited after the project end or preferable are already involved in the project at this current stage. They can be project partners or partners from the open call rounds already experienced in the implementation of symbIoTe. Every enabled IoT-Platform helps the adoption of the symbIoTe and the development of a sustainable solution in the long term.

6 Conclusions

Concluding the State-of-the-Art analysis of the IoT market, it can be stated that many different approaches are around for business models and based on different understanding. Looking on the different platform and project sites there are many interpretations of the term business model leading to various ways how the solution is made available to the community (e.g., open source, license based). A more detailed business model analysis builds CANVAS with the building blocks providing a broader view where the blocks channel and revenue stream fits the definition of business model most. Summarizing the analysis it can be stated that many things influence the selection of the business model, such are the application area and used hardware, as well as the availability of external sponsors, whether big providers are in included, whether development should be influenced by getting real life feedback, and whether there already is a final product placed on the market. Further impact on the business model selection has the purpose of the platform or services (e.g., home or office area, privacy support, data exchange). Having the combined CANVAS diagram (Figure 13) in mind it can be stated that symbIoTe combines all different channels and revenue streams that are mentioned by the identified platforms. Globally said, symbIoTe has a very complex business model that weights different items depending on the use-case and the goal of the responsible company.

The performed CANVAS proved that with development progress of the project symbIoTe more and more specific aspects are realizable. For each use-case a clear defined group of stakeholders could be identified where some common stakeholders can be found in all use-cases (e.g., symbIoTe consortium, hardware and software vendors, service providers). The cost structure is similar but clearly depends on the complexity of the use-case and the required equipment and maintenances. In addition, the revenue stream is similar favoring pay-of-usage and licensed fee scheme highly influenced by the envisioned use-case and the identified cost structure. Furthermore, it was identified due to CANVAS comparison that depending on the use-cases an offering of a combination of offerings as bundles seems to be more successful than offering them individually. The reasons for this observation is that different offerings require others to be in place before (e.g., secure communication and interoperability), in order to offer a promising service for an application. This main outcome will be further analyzed within WP7 focusing on exploitation.

Tussle analysis has been applied by many research projects in order to access socio-economic aspects of their technology and preclude unwanted effects when going to production [26,27,28]. This deliverable applied tussle analysis to all five use cases of symbIoTe. For the Smart Residence use case this showed that it will be important to develop a concrete action plan to convince residents, house operators, and small solution providers of symbIoTe. This support is necessary to overcome the resistance that is to be expected from large, monopoly-seeking smart home solution providers. Furthermore, it was shown that symbIoTe's strong focus on security is well justified. The EduCampus use case showed that concrete steps are necessary to convince key stakeholders of the symbIoTe solution. One of these key stakeholders are campus federations. As these federations exchange students frequently, they can be easily convinced of the advantages symbIoTe offers to them. For the Smart Stadium use case, the deployment of symbIoTe is in the interest of all stakeholders. In particular, the displaying of functionality will offer an additional revenue stream for stadium managers. Therefore, achieving a mainstream deployment of symbIoTe in stadiums or, more generally, public events, will be significantly easier. For the Smart Mobility and Ecological Routing use case the tussle analysis revealed questions that are mandatory to be answered by the symbIoTe consortium, in order to ensure that symbIoTe makes it to market. Also it was outlined why and how the symbIoTe solution can be misused to misguide individuals. Also it was shown that an individual's desire for long battery life collides with the common interest of having diverse measurement data. This constitutes a common dilemma and is out of scope for symbIoTe. No tussles were revealed for the Smart Yachting use case. As all stakeholders profit, when symbIoTe is deployed, getting the support of all key stakeholders is expected to be straightforward.

The use-case and show-case specific performed VNA empathized the findings of the CANVAS and Tussle analysis. The symbIoTe solution allows a very vast variety of applications with different business models in different industries. Thus, each application presents a vastly different value network with not only different stakeholders, but also different value streams between stakeholders existing in multiple show-cases in the same use-cases (i.e. Smart Stadium). This highlights the complexity of the symbIoTe solution and the difficulty to treat symbIoTe as one solution independent of use-cases and applications. For the Smart Resident use-case it showed the interoperability between different IoT-Platform providers and governmental platforms, i.e. for air quality. For the EduCampus use-case the value created for federated university campuses and their campus users got highlighted. In the Smart Stadium use-case the interoperability between different IoT-Platforms and platform providers was illustrated. In the Smart Mobility and Ecological Routing use-case it got demonstrated how the symbIoTe solution acts as link between all stakeholder’s platforms. Finally, in the Smart Yachting use-case the value network displayed how two different platforms create value when connected to a symbiotic network complementing each other.

The business model and sustainability recommendation is reflecting the findings of the previously summarized analyses. The complexity and differences between the use-cases would lead to an too unspecific model if they would been combined and, thus, be less useful. Therefore, individual recommendations are provided, customized to each use-case addressing the business model for the use-case and the sustainability aspects of at least one show-case. For the Smart Residence use-case a business providing its solutions based on the symbIoTe technology to home automation providers enabling platform interoperability is advised. A sustainable development could get achieved targeting small IoT-Platforms for application unionizing against big platforms. In the EduCampus use-case there are two possible options to be distinguished. Either one university is taking the lead and providing the symbIoTe service to other universities or an open-source community of joining university has to be build. In the first case, the hosting university would receive licenses from other universities and an access fee from third party service providers, in case the second show-case gets realized. In the second, each university hosts its own symbIoTe node and the community of universities is running the platform. Universities could make a profit of access fees for third party service providers. In order to create a network of university an initial base of members should join the network encouraging future members, i.e. universities participating in the symbIoTe project. In the Smart Stadium use-case the symbIoTe service provider would sell its services directly to the stadium and its manager. Further revenue streams could be reached by advertisement contracts for the promowall. For a sustainable development it is essential a company from the stadium infrastructure industry is enabling its platforms. Further should the managements and the users needs be met in order to provide a valuable added value. In the Smart Mobility and Ecological routing the symbIoTe operator receives revenue from the businesses using its mobility services and air quality data. In order to develop a sustainable platform local business should get attracted for creating revenue and incentivize local software companies in other cities to implement the symbIoTe mobility solution. In the Smart Yachting use-case it is advised a port IoT-Platform provider is providing the symbIoTe enable services to the port and receives revenue from the port management. The revenue could consist of a fixed maintenance part and a variable part for usage or service providers registered to the platform. In order to establish a sustainable platform it is advised to concentrate the marked entry effort in one defined area or high frequented travelling routes. This allows to raise awareness on the yachtsmen side and creates the need on the port side to include the symbIoTe enabled platform.

Summarizing the work of T1.2 with focus on Business Model and sustainability, it can be stated that for symbIoTe it is impossible to present one overall solution, because the assumed use-case show such a high diversity. Thus, the deliverable D1.5 presented for each of the five use-cases a specific analysis leading to individual business model recommendation and a list of sustainability items summarized in Chapter 5.

7 References

[1] D. Miorandi et al., “Internet of Things: Vision, Applications and Research Challenges,” *Ad Hoc Networks*, vol. 10, no. 7, 2012, pp. 1497–1516.

[2] R. Roman, J. Zhou, and J. Lopez, “On the Features and Challenges of Security and Privacy in Distributed Internet of Things,” *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266–2279.

[3] M. Machulak: *Protecting Personal Data in an IoT Network with UMA*. 3rd Kantara Initiative Workshop, Dublin, Ireland, Jun. 2014.

[4] D. Storm, “MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks,” *Computerworld*, 8 June 2015; www .computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical -devices-to-create-backdoors-in-hospital-network s .html.

[5] *Internet Security Threat Report*, Synantec Corporation Annual Report, 2013, www4.symantec .com/mktginfo/whitepaper/ISTR/21347932 _GA-internet-security-threat-report-volume-20 -2015-social_v2.pdf.

[6] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report, 2012; www.ftc.gov/ news-events/press-releases/2012/03/ftc-issues -final-commission-report-protecting-consumer, last visit Apr. 6, 2018

[7] Intel Developer Zone: Co*mmunication Patterns for the Internet of Things*. Jun. 1, 2016, URL: https://software.intel.com/en-us/articles/communication-patterns-for-the-internet-of-things, last access Apr. 6, 2018

[8] P. Darji: *A Simple IoT Taxonomy – Part 1*. SAP HANA Blog, Mar. 4, 2015, URL: https://blogs.saphana.com/2015/03/04/part-1-simple-iot-taxonomy/, last access Apr. 6, 2018

[9] C. Aggarwal, N. Ashish, and A. Sheth, “The Internet of Things: A Survey from the Data- Centric Perspective,” *Managing and Mining Sensor Data*, Springer, 2013, pp. 383–428.

[10] R.H. Weber, “Internet of Things—New Security and Privacy Challenges,” *Computer Law and Security Rev.*, vol. 26, no. 1, 2010, pp. 23–30.

[11] S. Zeadally et al., “Vehicular Ad hoc Networks (VANETS): Status, Results, and Challenges,” *Telecommunication Systems*, vol. 50, no. 4, 2010, pp. 217–241.

[12] J. Gubbi et al., “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” *Future Generation Computer Systems*, Elsevier, vol. 29, no. 7, 2013, pp. 1645–1660.

[13] N. Li et al., “Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey,” *Ad Hoc Networks*, vol. 7, no. 8, 2009, pp. 1501–1514.

[14] A. Osterwalder, Y. Pigneur, and C.L. Tucci: *Clarifying Business Models: Origins, Present, and Future of the Concept*. Communications of the Association of Information Systems, 16(1), 1, 2005.

[15] symbIoTe Deliverable D1.3 “Final Specification of Use Cases and Initial Report on Business Models”, published January 3, 2018, https://doi.org/10.5281/zenodo.817480

[16] A. Osterwalder: *The Business Model Ontology - A Proposition In A Design Science Approach.* PhD Thesis University of Lausanne, Lausanne, Switzerland, 2004.

[17] Strategyzer: *The Business Model CANVAS*, URL: http://www.businessmodelgeneration.com/canvas/bmc, last visit: Apr. 6, 2018

[18] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, A. V. Vasilakos: The Quest for Privacy in the Internet of Things; IEEE Computer Society, IEEE Cloud Computing, Vol. 2016, No. 3, pp. 34-43, April 2016

[19] C. Schmitt: IoT Connectivity vs Privacy Requests, Fifth SG13 Regional Workshop for Africa on "ITU-T Standardization Work on Future Networks: Towards a Better Future for Africa", Cairo, Egypt, April 1, 2017

[20] C. Schmitt: The Quest of Privacy, ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 2, ITU-T, Geneva, Switzerland, July 1, 2016

[21] Postscapes, https://www.postscapes.com/internet-of-things-platforms/#open-source-iot-platforms (last visit April 9, 2018)

[22] Deloitte: The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices, May 2014, https://tinyurl.com/deloitte-iot-ecosystem (last visit March 22, 2018)

[23] Mark Turck: Internet of Things: Are We There Yet? (The 2016 IoT Landscape). March 28, 2016, URL: http://mattturck.com/2016-iot-landscape/ (last visit April 14, 2018)

[24] Bosch: Internet of Things and Big Data: Vision and Concrete Use Cases. URL: https://www.slideshare.net/mongodb/internet-of-things-and-big-data-vision-and-concrete-use-cases (last visit April 19, 2018)

[25] D. D. Clark, J. Wroclawski, K. R. Sollins and R. Braden: *Tussle in cyberspace: defining tomorrow's Internet*, in IEEE/ACM Transactions on Networking, vol. 13, no. 3, pp. 462-475, June 2005.

[26] C. Kalogiros, I. Papafili, G. D. Stamoulis, C. Courcoubetis, G. Thanos, M. Waldburger, P. Poullie, B. Stiller, D. Field, M. Boniface, D2.2 - Final Report on Economic Future InternetCoordination Activities. SESERV Project, August 2012.

[27] ITU-T: Telecommunication Standardization Sector of ITU: Y.3013: Socio-economic Assessment of Future Networks by Tussle Analysis; ITU-T Recommendation Y.3013, August 2014.

[28] V. Burger, G. Darzanos, M. Dramitinos, Z. Dulinski, F. Faucheux, G. Hasslinger, F. Kaup, S. Kerboeuf, R. Lapacz, I. Papafili, P. Poullie, S. Randriamasy, M. Seufert, G. D. Stamoulis, R. Stankiewicz, M. Wichtlhuber, P. Wydrych, G. Rzym, K. Wajda: Report on Definition of Use-cases and Parameters, SmartenIT Project, August 2015.

[29] A. Sperroto, B. Naudts, B. Stiller, C. Tsiaras, C. Schmitt, D. Dönni, D. Tuncer, G. Machado, J. Serrat, J. Loyola, M. Charalambides, M. Flores, P. Poullie, R. Garg, R. Mijumbi, S. Uhlmann, S. Seeber, S. Verbrugge: D7.3 Economic, Legal and Regulative Constraints, FLAMINGO project, October 2015.

[30] Microsoft: Security Intelligence Report, Volume 9, Redmond, WA, USA, January 2010.

[31] Federation for EDucation in Europe, Geneva, Switzerland, http://www.fede.education, last accessed November 27, 2017.

[32] Universität Würzburg, Partner Universities, https://www.uni-wuerzburg.de/en/ueber/university/partnerunis/partnerunis-liste/, last accessed November 27, 2017.

[33] Universität Zürich, Strategische Partnerschaft mit der Freien Universität Berlin, https://www.int.uzh.ch/de/international/Strategische-Partnerschaften/Freie-Universität-Berlin.html, last accessed November 27, 2017.

[34] The Guardian, Google fined record r€2.4bn by EU over search engine results, online https://www.theguardian.com/business/2017/jun/27/google-braces-for-record-breaking-1bn-fine-from-eu, Last accessed November 28, 2017.

[35] symbIoTe Deliverable D5.2 “Report on System Integration and Application Implementation”, published August 30, 2017, https://doi.org/10.5281/zenodo.858836

[36] Independent advisory body of the European Commission on data protection issues - the Article 29 Working Party, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358 (last access May 6, 2018)

[37] EU Parliament: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (last access April 24, 2018)

[38] C. Battistella, K. Colucci, A.F. De Toni, and F. Nonino: Methodology of Business Ecosystems Network Analysis: A Case Study in Telecom Italia Future Centre. Technological Forecasting & Social Change, 80: 1194–1210, 2013.

[39] P. Ritala, V. Agouridas, D. Assimakopoulos, & O. Gies: Value Creation and Capture Mechanisms in Innovation Ecosystems: A Comparative Case Study. International Journal of Technology Management, 63(3/4): 244-267, 2013. http://dx.doi.org/10.1504/IJTM.2013.056900

[40] V. Allee: Reconfiguring the Value Network. Journal of Business Strategy, 21(4): 36-39, 2000. http://dx.doi.org/10.1108/eb040103

[41] M. Westerlund, S. Leminen & M. Rajahonka: Designing Business Models for the Internet of Things. Technology Innovation Management Review, 4(7): 5-14, 2014. http://timreview.ca/article/807

[42] V. Allee, "What is ValueNet Works Analysis?," in ValueNet Works Fieldbook, 2006.

[43] Information Commissioner’s Office (ICO; data protection regulator in the UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (last access May 6, 2018)

[44] Data Protection Directive 95/46/EC, October 24, 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en (last access May 6, 2018)

[45] N. Terrenghi et al.: Towards design elements to represent business models for Cyber Physical, Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018.

[46] EU Parliament: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1526910266966&uri=CELEX:32008L0050 (last access May 20, 2018)

[47] Board of Innovation, the icons for the VNAs are taken from the Business Model Kit. https://www.boardofinnovation.com/tools/. (last access May. 20, 2018).

[48] A. Bhatia , Z. Yusuf , D. Ritter , and N. Hunke: *Who Will Win the IoT Platform Wars?*, Boston Consulting Group, June 29, 2018. https://www.bcg.com/de-de/publications/2017/technology-industries-technology-digital-who-will-win-the-iot-platform-wars.aspx (last access Mai 25, 2018)

[50] R. Adner, R. Kapoor: *Value creation in innovation ecosystems: how the structure of technological interdependence affects firm performance in new technology generations*, Strategic Management Journal 31: 306–333, 2010.

[51] Cennamo, C. and Santalo, J. (2013), Platform competition: Strategic trade☐offs in platform markets. Strat. Mgmt. J., 34: 1331-1350. doi:10.1002/smj.2066

[52] MA. Schilling: Technology success and failure in winner☐take☐all markets: testing a model of technological lock out, Academy of Management Journal 45: 387–398, 2002.

[53] A. Gawer, MA. Cusumano MA: Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation. Harvard Business School Press: Boston, MA, 2002.

[54] symbIoTe Deliverable D1.2 “Initial Report on System Requirements and Architecture”, published September 30, 2016, https://doi.org/10.5281/zenodo.817465

[55] symbIoTe Deliverable D1.4 “Final Report on System Requirements and Architecture”, published July 17, 2017, https://doi.org/10.5281/zenodo.830156

8 Abbreviations

AAL	Active and Assisted Living
AIT	Austrian Institute of Technology
API	Application Programming Interface
ASA	AllSeen Alliance
AWS	Amazon Web Services
B2B	Business-to-Business
B2B2C	Business-to-Business-to-Customer
B2C	Business-to-Customer
BLE	Bluetooth Low Energy
BT	Bluetooth
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DSA	Distributed Services Architecture
DSLink	Distributed Service Link
EU	European Union
FP7	Forschungsrahmenprogramm 7
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GE	General Electrics
GSM	Global System for Mobile Communications
H2M	Human-to-Machine
H2020	Horizon 2020 program
HPE	Hewlett Packard Enterprise
IAQ	Indoor Air Quality
ID	IDentification
IDE	Integrated Development Environment
IO	Input-Output
IoT	Internet of Things
IP	Internet Protocol
ISOB	Fraunhofer - Institut für Optronik, Systemtechnik und Bildauswertung
ISP	Internet Service Provider

IT	Internet Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
L1	Level 1
L2	Level 2
L3	Level 3
LoRa	Long Range
LTE	Long Term Evolution
RFID	Radio Frequency IDentification
M2A	Machine-to-Analytic
M2D	Machine-to-Data-Lake
M2H	Machine-to-Human
M2M	Machine-to-Machine
M2P	Machine-to-Process
MPLS	Multiprotocol Label Switching
MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
NXW	Networks
OBU	On-Board Unit
OIC	Open Interconnect Consortium
OCF	OPEN CONNECTIVITY FOUNDATION
OSI	Open Systems Interconnection
OSGi	More exact: OSGi-Framework, Open Service Gateway initiative-framework: a framework to enforce strong modularization under java.
PaaS	Platform-as-a-Service
PbD	Privacy by Design
PETs	Privacy-Enhancing Technologies
PRISM	Planning Tool for Resource Integration, Synchronization, and Management
S&C	Sensing & Control Systems S.L.
SDK	Software Development Kit
symbIoTe	Symbiosis of smart objects across IoT environments
TA	Tussle Analysis
UC	Use-case

UPnP	Universal Plug and Play
URL	Uniform Resource Locator
US	Unites States
UW	UbiWhere
UZH	University of Zurich
VANET	Vehicular Ad Hoc Network
WSN	Wireless Sensor Network
VNA	Value-Network-Analysis
ZB	ZigBee

9 Appendix

9.1 EU General Data Protection Regulation (GDPR)

The finally approved EU General Data Protection Regulation (GDPR) [37] will replace the Data Protection Directive 95/46/EC [44] and will be enforced from May 25, 2018 on. It is designed to address the following items:

- To harmonize data privacy laws across Europe,
- To protect and empower all citizens data privacy in Europe, and
- To reshape the way organizations across the region approach data privacy.

The GDPR as well as its predecessor, the Directive, protects the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data.

According to the GDPR “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In addition, certain so-called special categories of personal data, such as religious or philosophical beliefs, data concerning health and biometric data are specially protected. Figure 36 shows examples.

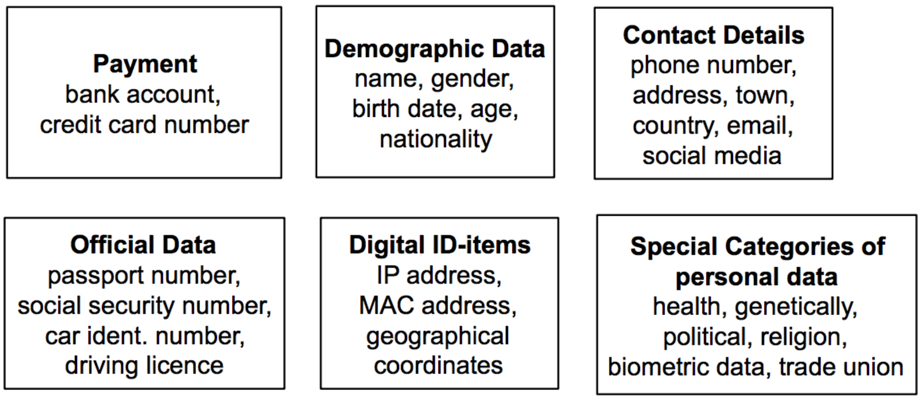

Figure 36: Examples of data worthy of protection

Examples of data not considered to be personal data are a company registration number, an email address such as info@company.com, and anonymized data.

The main highlights of the GDPR are summarized below [36, 37, 43]:

- *Exterritorial scope*
- *Tougher enforcement regime*: The GDPR introduces a tougher enforcement regime and it exposes companies to increased financial liability. Fines for non-compliance can be as severe as 4% of annual turnover or 20 million EUR – whichever is higher.
- *Strengthened data subject rights*: The regulation expands the existing rights for data subjects. Individuals will have the following rights:
    - Right to be informed (“transparency”),

  - Right to access,
  - Right to rectification,
  - Right to erasure (“right to be forgotten”),
  - Right to restriction of processing,
  - Right to data portability,
  - Right to object,
  - The right not to be subject to automated decision taking, including profiling.
- *Accountability and governance*, including keeping detailed records of processing and performing data protection impact assessments for high risk processing;
- *Data Protection Officer (DPO)*
- *Privacy by design and privacy by default*
- *Consent*
- *Data breach notification*: Introduction of a European wide requirement to notify data breaches to supervisory authorities and affected individuals.

9.2 Sustainability Motivation Graph

The applied methodology for creating a business model for connected cyber physical objects proposed by of Terrenghi, Schwarz and Legner [45] was used to create a stakeholder network and gather the motivations of each stakeholder. The method follows one string of interaction between the involved stakeholder. Following steps are taken to create the graph:

1. Define stakesholder need
   - In order to define the scope of your business model, start a scenario from the customer need
2. Identify essential stakeholders
   - In order to address a customer need, a collaborative network needs to be in place
3. Describe stakeholders interrelationships
   - Each stakeholder has a role in the network, defined by the type of value generated and received in it
4. Describe the benefits of each stakeholder
   - Stakeholders in the network should have clear advantages in taking their role

For each use-case one such graph was constructed leading to the mentioned results in Section 5.

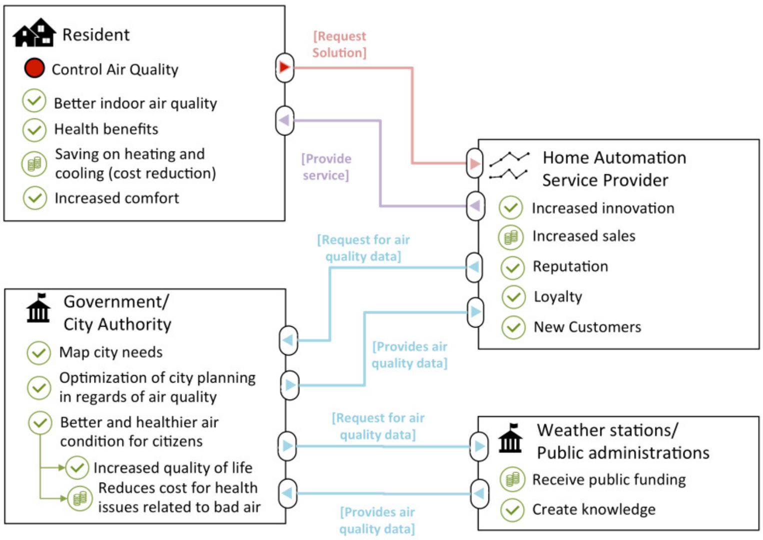

Figure 37: Smart Residence sustainability graph for show-case (1) on Healthy Indoor Air.

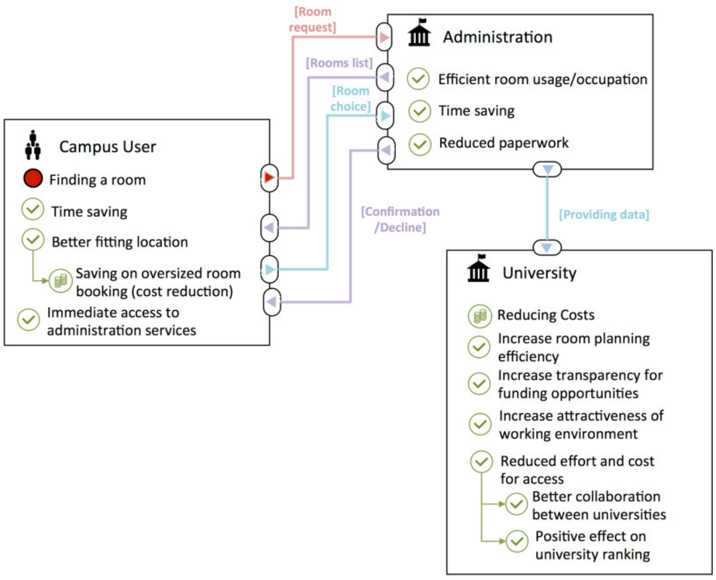

Figure 38: EduCampus sustainability graph for show-case (1) on campus federation.

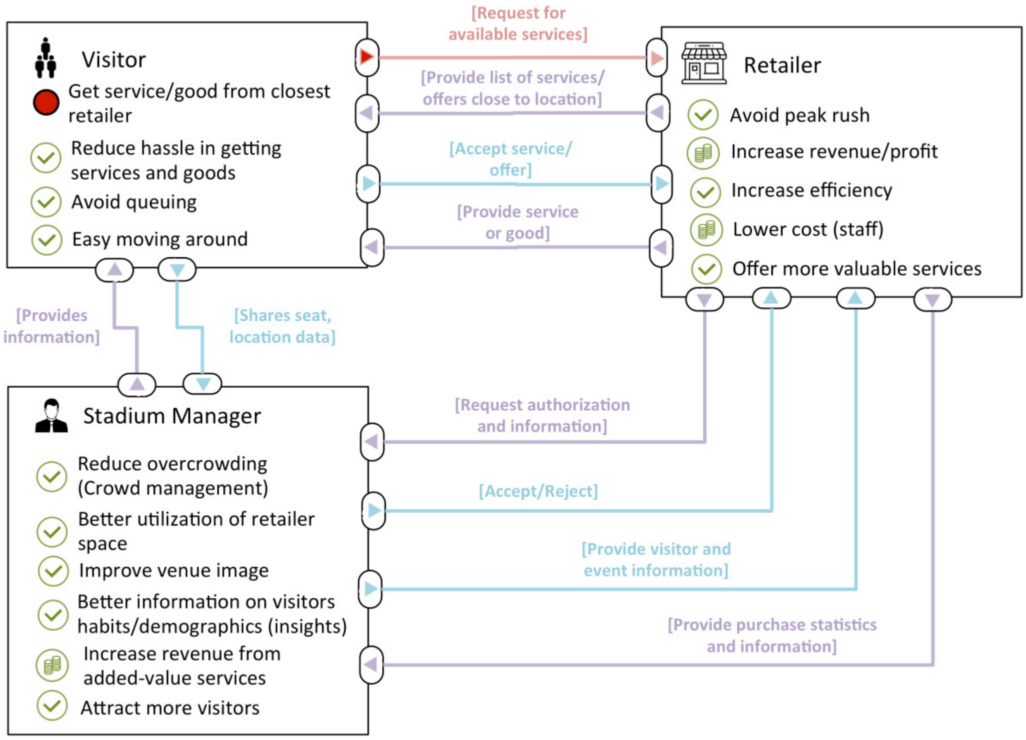

Figure 39: Smart Stadium sustainability graph for show-case (1) Vistor Application

.

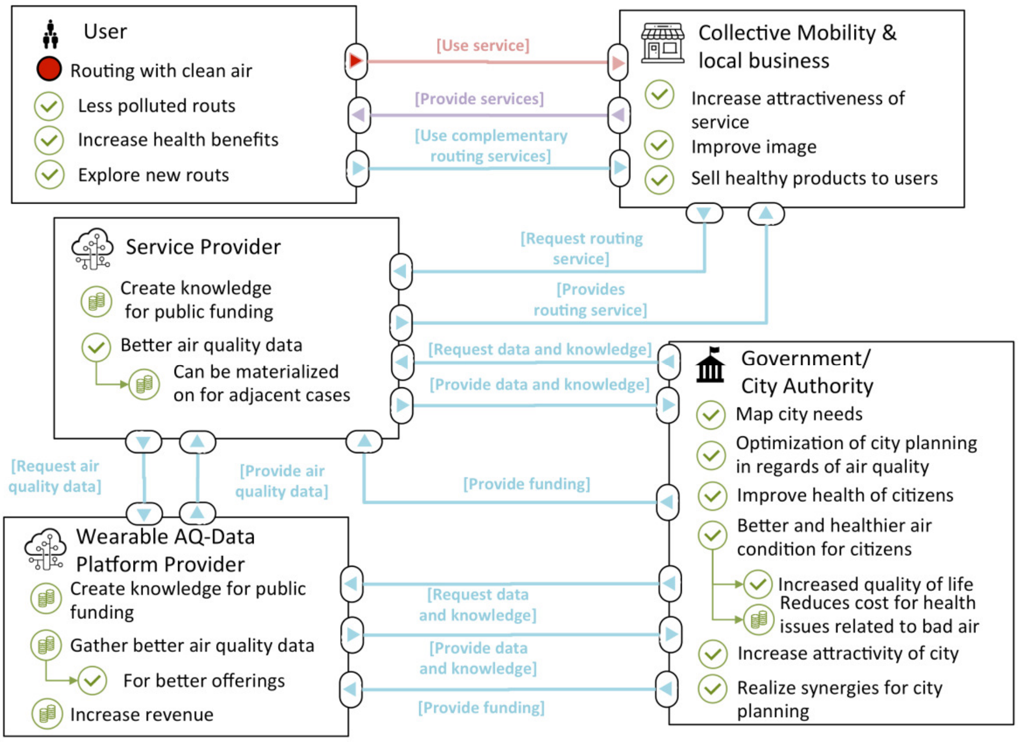

Figure 40: Smart Mobility and Ecological Routing sustainability graph.

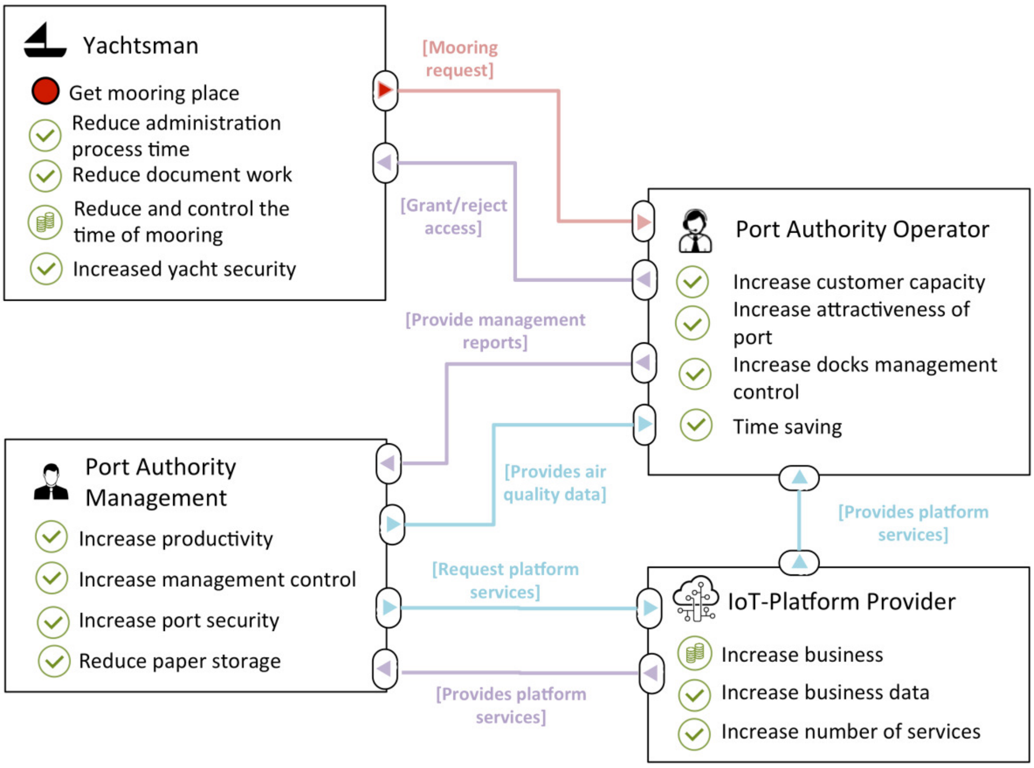

Figure 41: Smart Yachting sustainability graph for show-case (1) on Smart Mooring