Project Acronym:	SecureIoT
Grant Agreement number:	779899 (H2020-IoT03-2017 - RIA)
Project Full Title:	Predictive Security for IoT Platforms and Networks of Smart Objects

DELIVERABLE 7.2 - IoT Security Solutions Market Platform Architecture and Specifications_Final version

Deliverable Number	**D7.2**
Deliverable Name	**IoT Security Solutions Market Platform Architecture and Specifications_Final version**
Dissemination level	Public
Type of Document	Report
Contractual date of delivery	30/06/2019
Deliverable Leader	SiLO
Status & version	Final - v1.0
WP / Task responsible	WP7 (SiLO) / T7.1 (SiLO)
Keywords:	IoT marketplace, SECaaS marketplace
Abstract (few lines):	Detailed specification of the services of the market platform and of its architecture, based on T7.1.

Deliverable Leader:	George Boukis (SiLO)
Contributors:	George Angouras (SiLO), Apostolos Tsatsoulas (SiLO), John Soldatos (AIT), Giannis Kaldis (INTRASOFT)
Reviewers:	Daniel Calvo (ATOS), George Moldovan (SIEMENS)
Approved by:	Stylianos Georgoulas (INTRASOFT)

This document is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779899. It is the property of the SecureIoT consortium and shall not be distributed or reproduced without the formal approval of the SecureIoT Management Committee. The content of this report reflects only the authors' view. The Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information it contains.

Executive Summary

The purpose of this document is to describe the specifications and the architecture of the SecureIoT Marketplace, a Market Platform for IoT Security Solutions. SecureIoT Marketplace will be an entry point to accessing the integrated SecureIoT services and will provide access to the Exploitation Sandbox, a sandboxed environment that allows the easy testing of SecureIoT. Additionally, it will also provide relevant technical support, documentation and training capabilities. Therefore, SecureIoT Marketplace will serve mostly as an exploitation catalyst for the project and a common place for describing the SecureIoT SECaaS services.

The marketplace will be a Multi-Sided Market platform that offers to participants of the SecureIoT ecosystem marketplace related functionalities such as browsing and searching services, user registration, metering and accounting, but also will offer an entry point for finding integration and training services. Being a Multi-Sided platform means that there should be the ability to allow service providers to add their services and offer them through the SecureIoT Marketplace.

Based on these initial requirements and the analysis of relevant solutions, the specifications and the functionalities that the marketplace shall provide were described in the first version of this document (D7.1) [SecureIoTD7.1], along with an initial view on the architecture of the SecureIoT Marketplace. In this final version of the deliverable we provide the updated specifications, the marketplace roles and the final architecture of the platform based on the work done in the frame of task T7.1. This final version of the deliverable serves an update of D7.1 and will be the basis for the remaining efforts of WP7 tasks. It is important to state that reader should refer to D7.1 for a better understanding of the rationale for creating this marketplace, as both the relevant state of the art and the challenges identified remained unchanged since the creation of D7.1.

Document History			
Version	**Date**	**Contributor(s)**	**Description**
v0.1	07/05/2019	Angouras George (SiLO), Tsatsoulas Apostolos (SiLO)	Initial ToC
v0.2	13/06/2019	Angouras George (SiLO), Tsatsoulas Apostolos (SiLO)	Initial draft content added
v0.3	16/06/2019	George Boukis (SiLO)	Section 2.1 & 2.2
v0.4	17/06/2019	John Soldatos (AIT)	Section 2.3 and fixes in section 2
v0.5	21/06/2019	George Boukis (SiLO)	All sections ready
v0.6	24/06/2019	Giannis Kaldis (INTRASOFT)	Initial feedback on all sections
v0.7	02/07/2019	George Boukis (SiLO)	Ready for review
v0.8	05/07/2019	Daniel Calvo (ATOS), George Moldovan (SIEMENS)	Review
v0.9	08/07/2019	George Boukis (SiLO)	Addressed reviewers' comments
v1.0	11/07/2019	George Boukis (SiLO)	Final version to be submitted

Table of Contents

Executive Summary 2
Definitions, Acronyms and Abbreviations 8
1 Introduction 9
1.1 Scope and Purpose 9
1.2 Relation with other Work packages 9
1.3 Changes and Updates Since First Version 10
1.4 Document Structure 10
2 Market Platform Specifications 11
2.1 Stakeholders Overview 11
2.1.1 Reasons for a Multi-Sided Platform 11
2.1.2 Stakeholders of the SecureIoT Multi-Sided Platform 12
2.1.3 SecureIoT Market Roles and Provided Stakeholder Functionalities 13
2.1.4 Benefits that SecureIoT Multi-Sided Platform provides 13
2.1.4.1 Benefits for external stakeholders 13
2.1.4.2 Benefits for SecureIoT partners 14
2.2 Specifications of Core Market Platform Features 14
2.3 Liaisons and Integration with existing ecosystems 17
2.3.1 Alliance for IoT Innovation (AIOTI) (https://aioti.eu/) 17
2.3.2 Cluster of H2020 Projects on IoT Security 17
2.3.3 FAR-EDGE (www.edge4industry.eu) 18
2.3.4 IoT Catalogue (www.iot-catalogue.com) 18
2.3.5 IoT Platforms of the SecureIoT Partners (FIWARE, MindSphere, CloudCare2U) 19
2.4 Component and Services Offerings 19
2.4.1 Exploitation Sandbox Services 19
2.4.1.1 IoT Security Risk Assessment and Mitigation as a Service 19
2.4.1.2 IoT Compliance Auditing as a Service 20
2.4.1.3 IoT Developers Support as a Service 20
2.4.1.4 IoT Security Knowledge Base 20
2.4.2 Integration Services 20
2.4.3 Training Services 20

2.4.4 Business Support and Consulting Services 20
3 Market Platform Architecture 22
3.1 Conceptual Architecture of SecureIoT Marketplace 22
3.1.1 Scenarios 23
3.1.2 Logical View 23
3.1.3 Development View 25
3.1.4 Process View 26
3.1.5 Physical View 28
3.2 Base Technologies and Technical Solutions for the Implementation of SecureIoT Marketplace 29
3.3 Market Platform Development 30
3.3.1 SecureIoT Marketplace Implementation Status 30
3.3.2 SecureIoT Marketplace Sitemap 31
4 Conclusions and Next Steps 32
References 33

Table of Figures

FIGURE 1: 4+1 VIEW METHODOLOGY 22
FIGURE 2: THE FINAL VERSION OF HIGH-LEVEL LOGICAL VIEW OF THE SECUREIOT MARKETPLACE 24
FIGURE 3: HIGH-LEVEL DEVELOPMENT VIEW OF SECUREIOT MARKETPLACE– PACKAGE DIAGRAM 25
FIGURE 4: HIGH-LEVEL DEVELOPMENT VIEW OF SECUREIOT MARKETPLACE– PACKAGE DIAGRAM 26
FIGURE 5: MARKETPLACE REGISTRATION PROCESS 26
FIGURE 6: CREATION, VIEW, SUBSCRIPTION AND RATING OF A SERVICE 27
FIGURE 7: STAKEHOLDER MESSAGING IN THE MARKETPLACE 28
FIGURE 8: INDICATIVE DEPLOYMENT DIAGRAM OF SECUREIOT MARKETPLACE AND THE OFFERED SERVICES 29

List of Tables

TABLE 1: UPDATED TABLE OF PLATFORM FUNCTIONALITIES 14
TABLE 2: SCENARIOS FOR THE VALIDATION OF ARCHITECTURE 23
TABLE 3: PLATFORM FUNCTIONALITIES IMPLEMENTATION STATUS 30

Definitions, Acronyms and Abbreviations

Acronym	Title
AIOTI	Alliance for IoT Innovation
CTI	Cyber Threat Intelligence
CVSS	Common Vulnerability Scoring System
DoA	Description of Action
Dx	Deliverable (where x defines the deliverable identification number e.g. D1.1.1)
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IIoT	Industrial Internet of Things
IoT	Internet of Things
MSP	Multi-Sided Platform
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
R	Report
SECaaS	Security as a Service
SKB	Security Knowledge Base
WP	Work Package

1 Introduction

1.1 Scope and Purpose

The main goal of the SecureIoT project is to introduce, validate and promote a novel approach to the security of IoT applications, which emphasizes a timely, predictive and intelligent approach to the identification and mitigation of security threats and incidents. The project will create an architectural concept that can serve as the basis for implementing predictive and intelligent security systems and will also develop concrete security services that will be provided through the Security-as-a-Service (SECaaS) paradigm.

In this context, the purpose of the present deliverable is to describe the IoT Security Solutions Market Platform that is built in order to offer the aforementioned capabilities to interested stakeholders. Therefore, it will extend the results of SecureIoT for the purpose of better exploitation through the building of an appropriate community that will serve the sustainability strategy of the project.

The marketplace will be a Multi-Sided Market Platform (MSP) that will offer Security services on IoT based environments. For this reason, we investigated existing solutions in the fields of IoT platforms and how these platforms include the concept of the marketplace, and also examined marketplaces oriented to security and which offer SECaaS. The combination of these two different axes will offer to the SecureIoT a competitive advantage for the adoption of SecureIoT from relevant stakeholders.

Based on the findings of our research, but also based on the advancements on the technical work-packages of the project (WP3, WP4 and WP5), the specifications of the Marketplace are described in the document. Also, the initial services that will be included have been identified and documented. Main parts in the SecureIoT marketplace will be the offering of the SECaaS that will be developed and integrated into WP5, as well as the installation of an exploitation sandbox that will be part of the marketplace in order to provide a hands-on experience to the users.

In D7.1 [SecureIoTD7.1] the initial design of the marketplace has been produced, in order to allow us the development of the marketplace. As, between M12 and M18 of the project the development of the marketplace was active, this final version of the document provides the updates that were introduced in the architecture in order to allow for the realization of the platform. In this document the description of the architecture is provided as well, through the usage of multiple views that expose more details of the marketplace and assist the actual development of a platform.

1.2 Relation with other Work packages

The specification, design and implementation of the marketplace is a task that is based on the outcomes of the work-packages WP3, WP4 and WP5. Especially WP5 is really important as will provide the SECaaS that will be part of the Marketplace, while the components developed in WP3 and WP4 will be part of the exploitation sandbox. However, as the overall SecureIoT platform is under development, this document has been based mainly in the architectural designs that have been documented in deliverable D2.4 [SecureIoTD2.4] and early versions of D2.5[SecureIoTD2.5].

1.3 Changes and Updates Since First Version

As this deliverable serves as an update of D7.1, we provide here a comparison to deliverable D7.1, and highlight the updated sections in order to assist the reader of the document. In section 2, a new subsection (2.1.3) is introduced and explains the user roles needed for the marketplace creation, section 2.2 is updated with the identification of additional functionalities and the prioritization of them, while section 2.3 remained mostly unchanged. Regarding the architecture, section 3.1 was heavily updated as the logical view of architecture was updated and also is presented with more details, through the usage of more views and the introduction of short validation scenarios. Finally, section 3.2 includes only minor updates while section 3.3 has been added to provide a short overview of the marketplace development status. More details for the actual marketplace are provided in deliverable D7.7. It has to be stated that the relevant state of the art and the challenges identified remained unchanged since the creation of D7.1, so the user can refer to section 2 of deliverable D7.1.

1.4 Document Structure

The rest of the document is structured as follows:

- Section 2 described the specifications of the marketplace in terms of needed functionalities and also by describing the services that will be offered;
- Section 3 provides the architecture of the marketplace as part of SecureIoT and also provides some technical information on how we envisage the implementation of the marketplace, and also provides brief technical information about the marketplace development;
- Section 4 concludes the document.

2 Market Platform Specifications

2.1 Stakeholders Overview

One of the visions of SecureIoT is to design and develop a service-oriented ecosystem in a marketplace-like hierarchical structure concisely described in this deliverable as the "SecureIoT Market Platform". In this scope, it is important to gather the exploitable assets and the other "building block" components i.e.:

- tools, services, predictive security methodologies,
- schemes for risk assessment and compliance auditing,
- constructs for security data collection, security monitoring and predictive security mechanisms for smart object systems (of systems),
- info on relevant architectures,
- an explanatory knowledgebase that contains relevant publications, articles and blogs
- systematic access to business / technical support and consulting,
- detailed exhibits of hands-on use-cases (WP6),

as these are illustrated in WP2/WP6 and will be further elaborated in the deliverables of WP3-4-5 in a presentable and extrovert manner.

2.1.1 Reasons for a Multi-Sided Platform

It is envisioned that the integrated ecosystem will be able to provide a presentation of solutions and services in a coherent manner and become a means of evaluation of produced assets and results. These stretch over: security data collection, security monitoring and predictive security mechanisms, access to SECaaS, security simulation and assessment, compliance auditing, basic what-if-analysis, together with Predictive Security business consulting, technical assistance and/or training services. The main concept is their hierarchical presentation on top of other project related information and fundamental IoT and Security knowledge to various types of stakeholders.

The services of the SecureIoT ecosystem can be offered in the scope of "multisided platforms" (MSP) which in principle are technologies, products or services that create value primarily by enabling direct interactions among stakeholders or participant groups.

The scope of the ecosystem includes:

- An integrated platform to present the end results of SecureIoT in a coherent manner.
- A generic and modular MSP or even marketplace-like platform, including all the assets, services, offerings, knowledgebase and novel technologies employed on IoT Security by the project.
- To build an extensive multi-stakeholder community around it, that will assist in the dissemination and sustainability of SecureIoT.

- To attract a significant number of participants (critical mass) to its ecosystem and through this to increase the value offered to Security experts, IoT solution integrators and other relevant stakeholders.
- To provide a liaison point for similar initiatives with well-established related platforms existing communities and ecosystems, starting from communities where the partners are actively involved and to any similar ecosystems of the partners' such as research and commercial IoT, industrie4.0, Smart Infrastructure and Security platforms.
- The ecosystem should be a "presentation hub" while at the same time facilitating the sustainability, enhancement and improvement of the SecureIoT services following the end of the project's lifetime. The SecureIoT services and the ecosystem around them can become the core of the project's exploitation strategy.

2.1.2 Stakeholders of the SecureIoT Multi-Sided Platform

We distinguish between the following type of stakeholders;

Demand Side Stakeholders

These include: IoT & SEC integrators, IoT and Security vendors, Predictive security, SECaaS and Industrial/smart/IoT services developers, Risk assessment and compliance auditing specialists, IoT platform management specialists, affiliated business entities to partners, and all other stakeholders seeking novel security solutions and tools focused on IoT, participating in the ecosystem to learn about its assets, and to validate the functionalities and operations of associated products (Interfacing, Data Collection and Collaboration, Multi-Level Security Measures and Security Analytics, SecureIoT Services Implementation and Integration) from both a technical and a business perspective.

Supply Side Stakeholders

These include Consortium Partners as well as Third-party providers of IoT Security and SECaaS, on the broader spectrum of IoT applications, (SMEs, Researchers, Established ecosystems of businesses/research centres, affiliated business entities to SecureIoT partners, generic interested parties on similar cutting-edge technologies, etc). These should register and participate in the platform, and provide added value to it through offering reviews and ratings while conceptually also enhancing it as contributors of additional content and software modules that can form services together with SecureIoT offerings. Moreover, entities who have already achieved their own related implementations can certainly contribute/collaborate with their established work on Smart manufacturing and Industry 4.0, connected vehicle, Assistive Robot and e-health, or similar IoT/Smart environments, adding value to the project. Likewise, a contribution is expected by professionals on the broad security field.

2.1.3 SecureIoT Market Roles and Provided Stakeholder Functionalities

For the actual implementation of SecureIoT Marketplace, we identified specific roles that can be provided in order to provide support for the different type of stakeholders and also roles that were needed for the better management and support of the platform. The roles created in the marketplace are the following:

- **Visitor**, that is referring to the view that the marketplace is offering to unregistered users.
- **Marketplace Member (Customer)**, is the role that reflects the needs of the demand side stakeholders of the Marketplace. It allows register users to view and select services and at the same time allows the communication with the demand side stakeholders that offer services. Although in the scope of the project we will not provide support for payments, monetization is taken into account for the design of the platform and support for payments should be part of commercially exploited marketplace.
- **Manager**, is the role that encapsulates the additional functionalities that allow a user to add, edit and delete additional services in SecureIoT Marketplace.
- **Moderator,** is a role that is controlled by SecureIoT consortium members and allows the creation, editing or deletion of content that can be seen by visitors, customers and managers, as publications, blogs and news. The moderator also facilitates the management of all services created by Managers.
- **Administrator,** is also a role managed by the SecureIoT consortium and is focusing on the control of the users of the marketplace and the configuration of the platform.

More details about the functionalities and the pages that each of these roles can access is presented in section 3.3.2.

2.1.4 Benefits that SecureIoT Multi-Sided Platform provides

In this section we describe the added value that the Marketplace offers, in order to identify the functionalities that the marketplace shall offer.

2.1.4.1 Benefits for external stakeholders

The ecosystem should become a meeting place for developers, SECaaS specialists, Security Consultants, IoT decision makers, relevant service providers, broader IoT services developers, e-health, smart transportation, Industry4.0 or other IoT-related integrators, as well as professionals on the legal/technical/business aspects of security application, assessment and compliance, and finally OEMs, SMEs, Researchers and other related stakeholders. The systemized nature of a participatory ecosystem focused specifically on IoT Security is deemed to be the utmost advantage of creating a critical mass of the community since the topic is novel and insufficiently addressed. Moreover, this ecosystem will enable stakeholders to benefit from the specific services of the project, learn about them, evaluate them and ultimately (hopefully) augment them through contributions and collaborations at a later stage.

2.1.4.2 Benefits for SecureIoT partners

The ecosystem should constitute a focal point of gathering results, innovations, services, and an extensive knowledge base of articles, training material, consulting/support material and use-case applications.

Other (similar or affiliated) IoT/ SEC / SECaaS applications and deployments by external supply-side stakeholders or by related projects and ecosystems can feature many cross-platform and cross-vertical interactions. Through stakeholder interaction and even evaluation of offered services by external stakeholders, the process should enable partners to constantly improve SecureIoT tools and services features.

Moreover, following the establishment of an ecosystem around the project's results, the project will pursue a number of exploitation (or even consider monetization) modalities that would allow the consortium to sustain and gradually expand the scope of the ecosystem as these will be analysed in WP8.

2.2 Specifications of Core Market Platform Features

After identifying the challenges that a Multi-Sided Marketplace for IoT Security will have to address and by researching on relevant solutions, the specifications for the marketplace have been described in D7.1. After the submission of D7.1, SiLO and AIT initiated the development of the marketplace, in the scope of task T7.4: Multi-Sided Market Platform Realization. During this period, we also went through the specifications and the required functionalities that they generated, tried to prioritize the implementation of them and also tried to identify specifications/functionalities that haven't been initially planned.

The following table illustrates some of the core functionalities and features that the ecosystem should include. The first version of the specifications table was provided in D7.1, and in this final version we updated the specifications by adding one additional specification, based on the feedback collected from demonstrating the existing functionalities to the consortium partners. Also, based on this collected feedback we provided priorities to the specifications. Functionalities assigned with High priority are either considered critical for the functioning of the marketplace or are critical for achieving the goals of SecureIoT. Functionalities assigned with Medium priority are considered important for creating a successful platform but are not so critical and therefore can be implemented in later stages. Functionalities with Low priority are not considered as important at this stage and will not be implemented during the project's duration.

Table 1: Updated Table of Platform Functionalities

MSP Ecosystem Functionality	Short Description	Priority
Specifications from D7.1		
Registering Participants & Business Entities	Registration of participants to the ecosystem	High

Authentication and Authorization	Ensuring authenticated and authorized access to the various services and sections of the platform	High
Search and discovery of service offerings	Search engine for discovering available services based on appropriate metadata for the descriptions of the services	Medium
Catalogue Publishing of services	Publication and presentation of the ecosystem services, solutions, tools, and other entities described in WP2	High
Provision of recommendations	Context-aware proposition of relative service offerings	Medium
Collaboration Services	Collaboration Services (e.g., Forum / Messaging / Repository), including the relevant community support	High
Review and rating of service offerings	Tools for rating service offerings from the end-users / participants viewpoints	Medium
Manage and tracking registered services	Access to the status of subscriptions and services	High
Solution Presentation	Solution presentation through examples	High
Services Presentation	A comprehensive list of all services described in WP6	High
Knowledge base	Information Services including articles, presentations, News, Blog etc. On-line training and education services in the form of self-contained presentations	High
Marketplace Layout	Aggregation of Services and Solutions in categories/subcategories with searchable metadata, thumbnails, descriptions, ratings. Management features for addition/deletion/categorisation etc.	High
Future Monetisation Module (marketplace / e-commerce)	Pricing scheme (per unit/service/data volume/usage units or freemium). Also, the welcome addition would be to provide e-commerce / secure transaction management through 3rd party integration	Medium
Libraries	Middleware libraries for SEC, SECaaS and general IoT, as well as open APIs for accessing the libraries including accompanying documentation	Medium
Developers' support services	Developers joining the project's platform will be offered with access to APIs and annotations and a dedicated IoT Developers Support as a Service function	High
Training, consulting and	These services will be offered in the form of complementary (augmented) added value services	High

technical support services	through partner value chains (expert human interface needed)	
Access to Services	The ability for stakeholders to use, evaluate and consider the use of the: -IoT Security Risk Assessment and Mitigation as a Service -IoT Compliance Auditing as a Service - IoT Programming Support Services - IoT Knowledge Base - Relevant regulations and directives knowledgebase (e.g. GDPR, NIS, ePrivacy)	High
Access to Tools	Coherent presentation and access to code produced by the project on the topics of: -Interfacing, Data Collection and Collaboration -Multi-Level Security Measures and Security Analytics -SecureIoT Services Implementation and Integration (SECaaS)	Medium
Use Case Paradigm Presentation	End to end implemented solutions serving as an example of integration: (smart manufacturing -Industrie 4.0, connected cars and IoT-enabled socially assistive robots)	High
Localization	Support for an international environment through appropriate localization of the services including currency and language support	Low
New Specifications		
Registration through 3rd party authentication services	Support for authentication with 3rd party services such as Google or LinkedIn as this is some users prefer this for faster registration.	Medium
User and Organization Management	The ability to manage organizations and users participating in an organization	Medium
Basic Content Management Support	Provide content (publications, news, blogs etc) for visitors. Content should be editable by the moderator	Medium
Support of Privacy and Security Regulations	Critical user and service data will be stored encrypted and secure connection SSL/TLS will be used. Privacy policy compatible with GDPR shall be created, taking into account the legal rights of the registered users (e.g.: right to be informed, right to be forgotten), rules for long term storage of the data, and the specification of contact points for users of the platform.	High

From the identified functionalities, only the *Localization*, is not considered important to be implemented in the scope of the project duration, while all other functionalities should be implemented.

2.3 Liaisons and Integration with existing ecosystems

The success of such ventures is largely dependent in the attraction of a significant number of participants (critical mass) to its ecosystem because it is generally accepted that the size of the community is the predominant metric for sustainability. In order to increase exposure, SecureIoT will try to liaise with renowned business partners of the consortium partners, will try to offer its augmented security services to existing already established communities and ecosystems, starting from communities where the partners are actively involved and to the IoT ecosystems of the partners' commercial platforms. Special emphasis will be paid in the study of the **business motivation** of enterprises to participate in the SecureIoT ecosystem for better targeting and hence more efficient penetration.

This leads to the conclusion that apart from the evident need for an internal web **portal,** obviously further augmented with a **participatory collaboration** platform and with a **specialized marketplace** which could even lead to monetization, for SecureIoT to have as a basis for its ecosystem, the following complementary alternatives are considered as deployment and implementation candidates for the SecureIoT Ecosystem platform and the presentation of the project service offerings. These constitute "affiliated" ecosystems that are already launched and have started their community building efforts. In particular, synergies with the following ecosystem platforms and communities will be considered:

2.3.1 Alliance for IoT Innovation (AIOTI) (https://aioti.eu/)

The AIOTI brings together prominent IoT stakeholders around Europe, which collaborate and exchange information in order to foster the development of the European IoT ecosystem. AIOTI is structured in several working groups, which include groups that focus on IoT vertical applications. SecureIoT has very strong links with AIOTI in general and some of its working groups (e.g., WG11 on Smart Manufacturing), where partners (e.g., AIT, FUJITSU, SIEMENS) participate with a leading role. Therefore, the project will establish a close collaboration with AIOTI as part of its effort to attract stakeholders in each ecosystem platform. As a prominent example, SecureIoT will invite AIOTI participants to contribute data-driven security monitoring algorithms to the SecureIoT market platform. As another example, AIOTI members will be invited to access demonstrations of the SecureIoT SECaaS services by providing access to proper datasets of their platforms and devices.

2.3.2 Cluster of H2020 Projects on IoT Security

SecureIoT is part of a cluster of research and innovation projects on IoT security, which are funded by the European Commission and its H2020 programme while running in parallel. Apart from SecureIoT, this list of projects includes H2020 ENACT, IoT Crawler, SEMIOTICS, CHARIOT, SOFIE, CREATE-IoT and Ser-IoT. Furthermore, recently a new Coordination and Support Action (CSA) has been created, titled NGIOT: Internet of Things for Research Leadership and Global

Competitiveness (IOT4EU)[1] coordinating the activities of these projects. SecureIoT will share and exchange information, algorithms and security approaches will all these projects. As a follow up of these activities, some of the information shared can serve as a basis for the supply side content of the SecureIoT market platform. At the same time, members of this community can become demand-side members of the market platform, especially during the early stages of the SecureIoT ecosystem development, where we will seek to bootstrap the community fast and with a relatively small budget for community building activities. SecureIoT's collaboration with these projects will, therefore, include presentations of the market/ecosystem platform during meetings and other events organized by the cluster of these projects and the IoT4EU CSA.

2.3.3 FAR-EDGE (www.edge4industry.eu)

The H2020 FAR-EDGE project has recently (June 2018) launched its ecosystem portal platform, which provides access to all its digital automation solutions. The project's is currently undertaking intense community-building efforts, which are attracting registered participants beyond the project's communities (i.e. third parties). FAR-EDGE and the Edge4Industry community are very pertinent to Secure IoT, as they both include security mechanisms for IoT/IIoT, the main difference being that security is a core topic of SecureIoT and an auxiliary/support theme in FAR-EDGE. Therefore, there are good reasons for SecureIoT to pursue collaboration and joint community building efforts with FAR-EDGE. Likewise, SecureIoT will consider linking its ecosystem and/or results to the FAR-EDGE ecosystem portal, as a means of achieving multiplier effects for the community building efforts of both projects (e.g., providing SecureIoT content and services to registered participants of the FAR-EDGE ecosystem).

2.3.4 IoT Catalogue (www.iot-catalogue.com)

The IoT Catalogue provides a single access point to several IoT-related results from EU projects and beyond. The platform acts as a marketplace, which provides product/catalogue services in the IoT domain. All SecureIoT results, specific know-how, components and services definitely fall in the realm of the Internet of Things spectrum with the added benefit of addressing the cutting-edge subject of security, and therefore could find a place in the IoT Catalogue. Moreover, the IoT Catalogue is a product of an established institute with a long history of collaboration with several SecureIoT project partners, which can obviously facilitate relevant integration efforts and synergies. As a result, SecureIoT results could be hosted in the IoT Catalogue. While this will ease the project's marketplace and MSP development efforts, it will deprive the project of the opportunity of developing its own brand/marketplace critical mass. This trade-off between ease of development and potential lack of branding will be evaluated and resolved as part of the project's ecosystem and marketplace development efforts in the following WPs. We hence envision this as a complementary action for added participator numbers and fast-track exposure. Examples include the possible demonstration (and future monetization) of:

- Seas Modules

[1] https://www.ngiot.eu/

- IoT Security Knowledge Base
- Integration Services as part of the Marketplace
- Training Services as part of the Marketplace
- Business Support Services as part of the Marketplace

2.3.5 IoT Platforms of the SecureIoT Partners (FIWARE, MindSphere, CloudCare2U)

The SecureIoT partners will liaise with communities and stakeholders associated with the main IoT platforms that are used in the project, namely FIWARE, MindSphere and CloudCare2U. Apart from the obvious boost, the project's community-building efforts, such as a liaison could result in a set of new assets and demonstrators of SecureIoT results, which will be targeted to the users of these platforms. For example, SecureIoT algorithms could be used to provide a service for risk assessment of devices attached to any of these platforms.

2.4 Component and Services Offerings

Here we provide the list of services or components that the marketplace will offer, with services include the SECaaS services developed in WP5, but also others like technical support services, integration services, training services, business support services etc.

2.4.1 Exploitation Sandbox Services

SecureIoT will provide a pool of SECaaS services under an exploitation sandbox that will be part of the SecureIoT market platform. The goal will be to demonstrate SECaaS results in controlled environments and at a quite limited scale, as a means of illustrating the project's results to the SecureIoT community. Examples of SecureIoT services that could be delivered as cut-down versions in a sandbox environment include:

- IoT Security Risk Assessment and Mitigation as a Service,
- IoT Compliance Auditing as a Service
- IoT Developers Support as a Service
- Other SECaaS solutions

A brief description of the services that will be considered for deployment in the SecureIoT's sandbox environment follows.

2.4.1.1 IoT Security Risk Assessment and Mitigation as a Service

The Risk Assessment and Mitigation Service (RAM) will produce an assessment calculation of potential risks and propose mitigation actions such as security policies. The service will take advantage of knowledge derived based on Data Monitoring & Analytics component of the SecureIoT Architecture and the NIST's Common Vulnerability Scoring System (CVSS). The service will quantify risks in terms of a "likelihood factor", which will be calculated based on a combination of the probability and impact of any identified vulnerabilities. For the configuration and presentation of the service GUI and visual tools will be offered.

2.4.1.2 IoT Compliance Auditing as a Service

The Compliance Auditing Service will be delivered as a tool available to solution deployers, operators and end-users. It will provide support for a set of security and privacy controls on the IoT infrastructures at multiple levels. The auditing will provide recommendations about areas that require attention, while automatically enforcing policies where/when needed. More specifically, this service will evaluate compliance with controls specified by relevant regulations, standards, good practices, etc. Compliance Auditing will involve data usage across the layers of the SecureIoT solutions. Cross-Layer Data Exchange will facilitate the modularity of a solution and supports evaluation of compliance using data from various layers.

2.4.1.3 IoT Developers Support as a Service

The Developer Support Service will assist IoT developers to secure their applications by using programming annotations and deployment descriptors. This service will enable the developers at design time to plan the enforcement of policies at run-time. The provision of this service will not be limited to offering a runtime infrastructure and accompanying tools for visual development. Rather comprehensive documentation, along with online support services will be offered as well.

2.4.1.4 IoT Security Knowledge Base

The SecureIoT architecture introduces an IoT security knowledge base component, which can be used to match identified abnormal or suspicious behaviours with known vulnerabilities or attacks. The Security Knowledge Base (SKB) will store structured information on threats including, but not limited to CPE, CWE, CVE and CAPEC specifications as Cyber Threat Intelligence (CTI) sources. CTI will also be able to enhance other components of SECaaS through an API.

2.4.2 Integration Services

As part of the marketplace offerings, integration services will be offered through SecureIoT. A service provider will be able to register to SecureIoT and describe with details the integration service he/she offers. The end user then will be able to read and also compare the available services and decide to communicate with the service provider for the actual usage of the service.

2.4.3 Training Services

Another important offering of the SecureIoT marketplace is the ability to provide training services. Training services will include documentation in terms of tutorials for self-training and questionnaires for self-assessment, but will also allow third parties to register as training service providers that can provide training sessions to interested users.

2.4.4 Business Support and Consulting Services

SecureIoT Marketplace will also provide the ability to host services for business support and consulting. Similarly, to the integration services, the service provider will register to SecureIoT Marketplace and describe the service he/she offers. The end user then will be able to read and also compare the available services and decide to communicate with the service provider for the actual usage of the service.

3 Market Platform Architecture

In this section, we present the architecture of SecureIoT Market Platform. The vision of SecureIoT is to implement a Multi-Sided Platform (MSP) for IoT-based cyber-security solutions, based on the identified specifications and will be a single-entry point for SecureIoT's open standardized cyber-security services (i.e. risk assessment, compliance auditing, developers' support).

The SecureIoT overall architecture has been presented in deliverable D2.4 and is destined to support a security platform that will deliver SECaaS services to various IoT systems/platforms. The SECaaS services will be offered to different IoT systems that provide their data to the SecureIoT services provider i.e. the entity that is deploying and operating the SecureIoT platform. This approach covers one side of the platform, the users of the services. The other side of the platform is enabled by the SecureIoT services providers that deliver to IoT systems owners or operators services such as Risk Assessments, Compliance Auditing and Developers' Support, along with a range of security automation (e.g., alerts) and visualization services (e.g., display of information in dashboards).

3.1 Conceptual Architecture of SecureIoT Marketplace

By following the same approach with deliverable D2.4 that provides the overall architecture of SecureIoT using multiple views, according to the "4+1" views methodology [Kruchten95], the architecture of SecureIoT Marketplace is defined. By "4+1" views methodology, the architecture is described based on four complementary views; logical view, process view, development view and physical view. These views are complemented by a set of specified scenarios and use cases, which are used to validate the architecture.

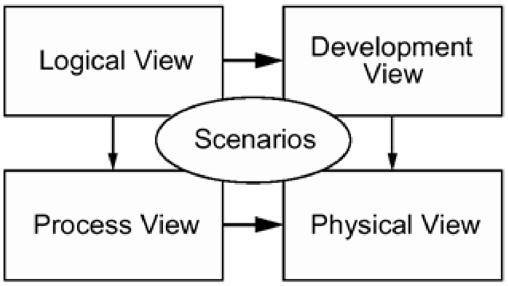

Figure 1: 4+1 View Methodology

The logical view depicts the high-level view of the architecture, including its main components and the way they are structured together, this is the initial view that actually drives the specification of the development. Following the specification of the logical view, a development view can be derived and elaborated in order to provide insight on the implementation task of the architecture, while a process view can be also elaborated in order to show the dynamic behaviour of the system, including interactions and information flows between the various components. Finally, the physical view provides insights on the physical implementation and deployment of a system that is based on the specified architecture.

3.1.1 Scenarios

Although in D2.1 scenarios have been defined for SecureIoT, these scenarios were related mostly to the security needs of the use cases and drive the development of the SECaaS, and are not specific for the marketplace usage. Based on the State-of-the-Art analysis and the specifications that were already collected in D7.1, we tried to produce a few simple scenarios that can help on the validation of the marketplace platform. These scenarios are very closely related to the specifications and the corresponding functionalities that have been produced and prioritized above, and are actually covering the most important functionalities of the platform. Therefore, the main reason for producing these scenarios is to provide specific actions for validating the architecture and in later steps, the developed marketplace platform, and also to help us define the process view of the architecture.

Table 2: Scenarios for the validation of architecture

ID	Scenario Name	Description
MS1	MSP Registration	Allow users to register on the platform with multiple roles
MS2	Usage of Services	Demand-side stakeholders can view the available services and learn how to use them
MS3	Register Services	Supply-side stakeholders can register and edit services that demand-side stakeholders can use
MS4	User Management	Administrator is able to accept, edit or delete a user
MS5	Content Management	Moderator is able to edit content that is presented to visitors
MS6	Customer Communicates with Seller	A demand-side stakeholder should be able to communicate with the supply side stakeholder offering a service.
MS7	Users communicate and discuss	Users of the platform use forum to communication
MS8	Customers select and rate services	A demand-side stakeholder should be able to rate a service

3.1.2 Logical View

In D7.1 we provided only the logical view, as the most important view of the system. In this deliverable we provide an updated version of the logical view, and in the following figure the conceptual architecture of SecureIoT Marketplace is provided.

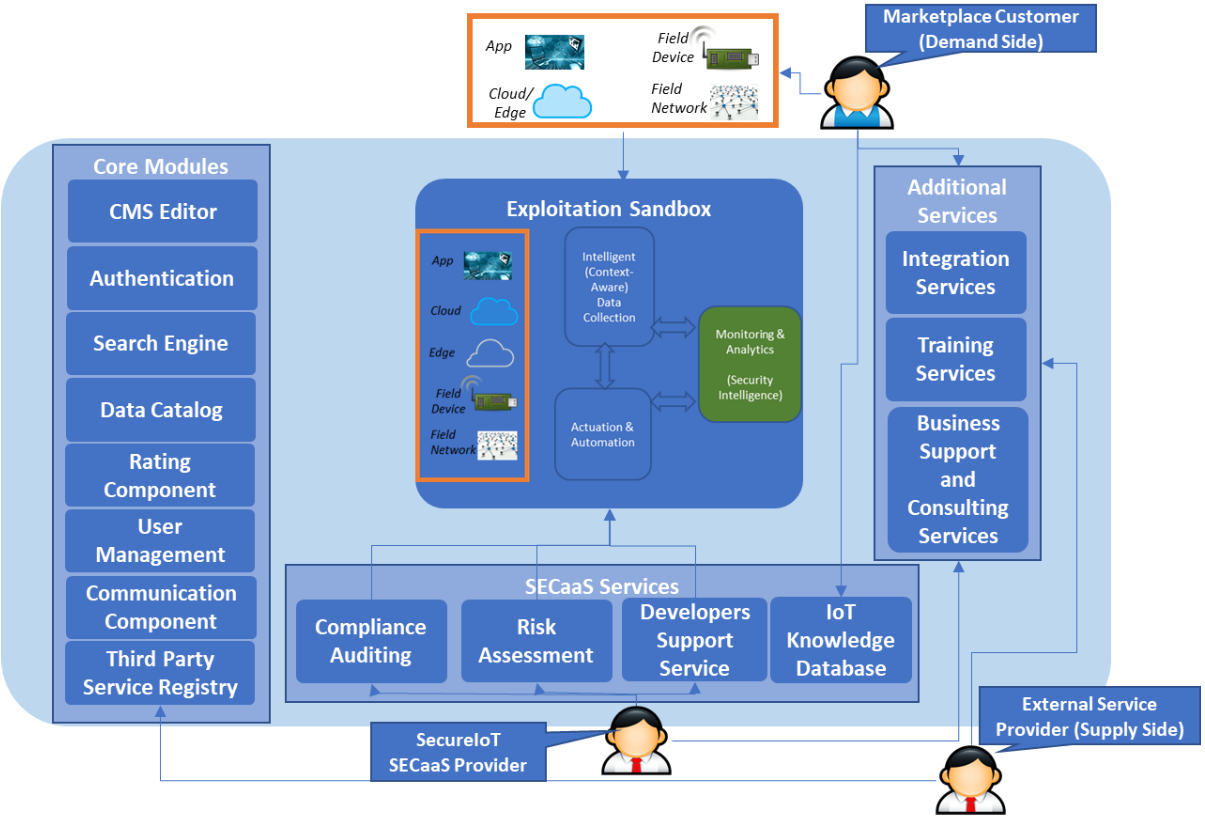

Figure 2: The final version of High-Level Logical View of the SecureIoT Marketplace

In this logical view, the main layers can of the marketplace are the following:

- **Core Modules:** Core modules layer includes all the components of SecureIoT Marketplace that implement the core marketplace functionalities. It includes modules for data catalogue, search, rating and authentication. In the updated version it includes modules for user management, communication between the users (messaging and forum), and also a Content Management Component (CMS Editor). It also includes an add-on module that is responsible for the connection to any third-party service.
- **Exploitation Sandbox:** the exploitation sandbox is a part of the marketplace dedicated to offering to interested end users of the market an easy way to connect and use SecureIoT for testing in a sandboxed environment. The sandboxed environment will provide the possibility to use it as is for understanding the platform, or to connect own devices and datasets for more concrete testing. It also provides the possibility to use SECaaS that already deployed with the sandbox environment.
- **SECaaS Layer:** SECaaS layer includes the security services created in WP5. These services are available in two different forms; a) through the exploitation sandbox b) by providing description, instructions and needed artefacts for their standalone usage.
- **Additional Services:** Additional services that represent integration services, training services and Business support or consulting services are also provided. These services are having no direct connection to SecureIoT or the developed SECaaS but can be beneficial

to the users and important for the adoption of SecureIoT. These services can be added by the SecureIoT consortium or third parties connected to the SecureIoT marketplace.

3.1.3 Development View

A high-level development view of the marketplace architecture has been created during this period and is depicted in the component diagram of Figure 3 and also in Figure 4 that complements the component diagram with the database entities. The component diagram presents the components need for creating the Marketplace. For this presentation we have clustered together modules that have similar functionalities, such as the *Service Registry* Controllers (that rely on a single base interface and include the SECaaS Controller, the Business Services Controller and the SecureIoT Solutions Controller) and the more generic *Marketplace Backend Services* that includes Data Catalog, Search, Rating, Subscription, Monetization and Direct Message Services.

The diagram explains also the dependencies between some modules through identifying modules that use other modules. This way we present how the *User Interface* of the Marketplace depends on the *Web Controllers* and *User Management* modules, and how these modules use the available modules that form the backend of the marketplace.

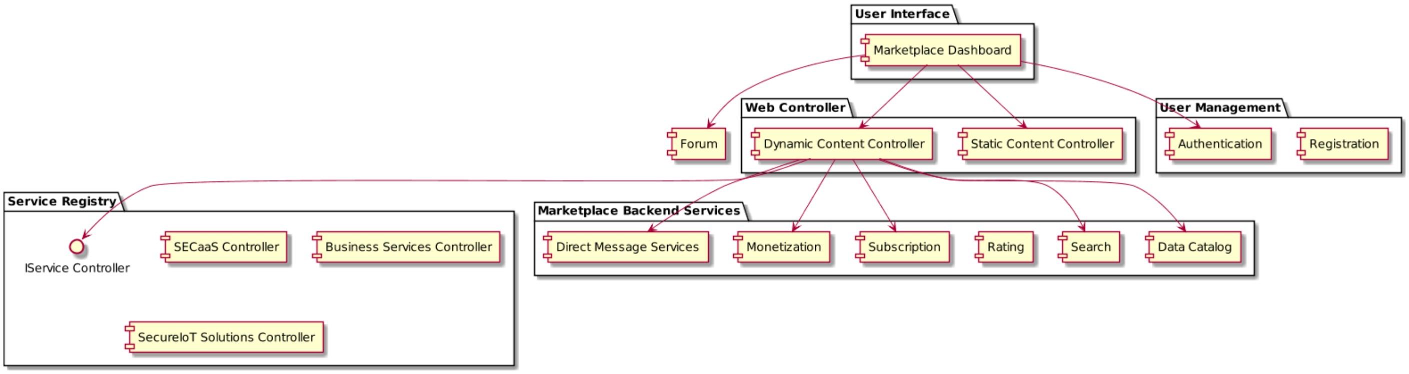

Figure 3: High-Level Development View of SecureIoT Marketplace– Package Diagram

The components that are part of *Service Registry*, *Marketplace Backend Services* and *User Management* packages rely on a relational database for the persistent storage of the data of the marketplace. The required entities of the database are depicted in Figure 4 below.

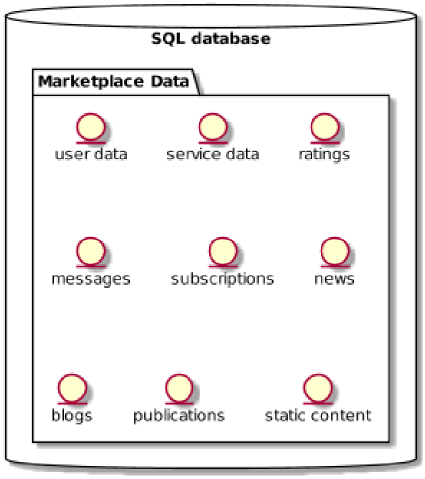

Figure 4: High-Level Development View of SecureIoT Marketplace– Package Diagram

3.1.4 Process View

The sequence diagrams of Figure 5 and of Figure 6 and Figure 7 depict three important sample processes of the MSP marketplace (registration and user management, service registration and presentation, messaging), and how these processes are implemented through the communication of the components presented in the logical view of the architecture. In particular, in Figure 5 we view the registration process of a new stakeholder, that can be a Customer (demand side stakeholder) or Manager (supply side stakeholder). In this view we see that the administrator of the platform controls the whole process and that the *Dynamic Content Controller* is used to provide user-specific content to the registered users.

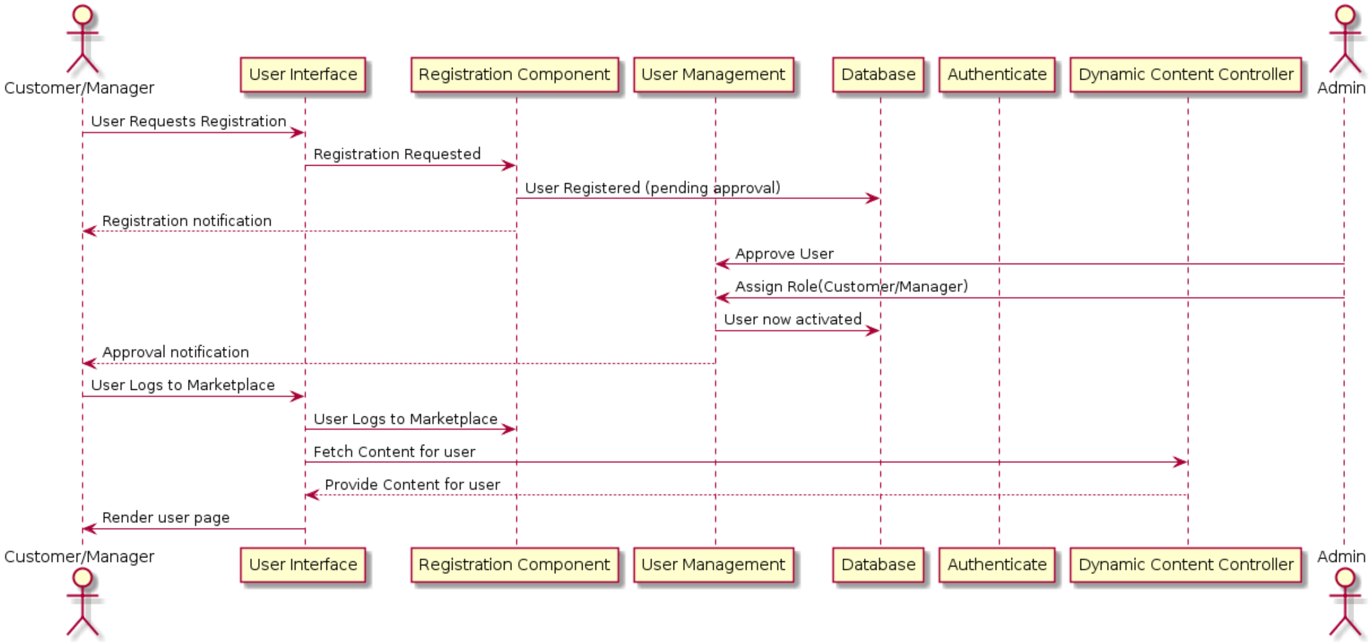

Figure 5: Marketplace Registration Process

In Figure 6, we present a complex process that can be actually split into 4 different logical steps that present different sub-processes; **a)** Manager registers a Service (a SECaaS in this example), **b)** Customer Views the Service, **c)** Customer rates the service, and **d)** Customer subscribes to service. Each of these sub-processes relies on different components of the marketplace.

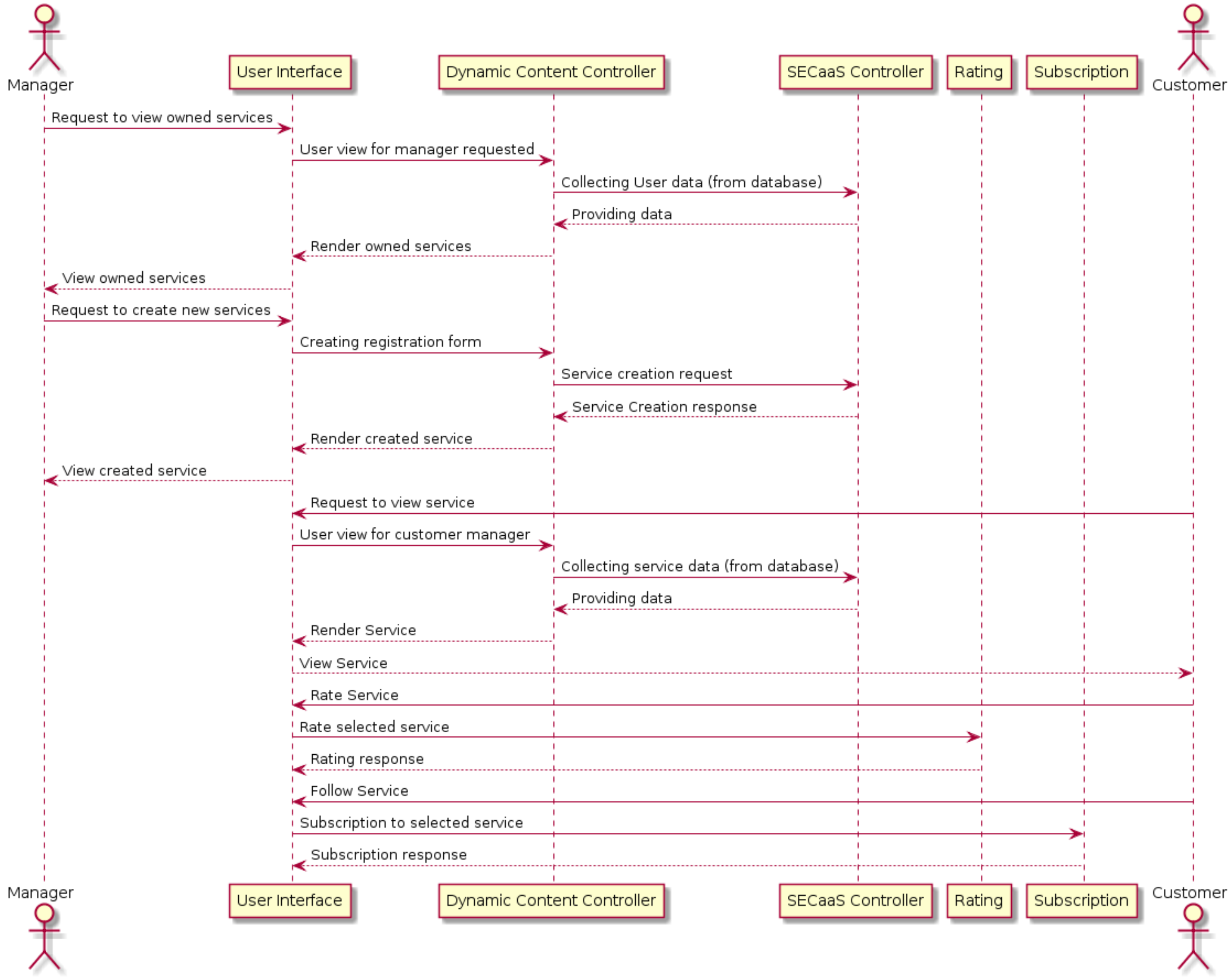

Figure 6: Creation, View, Subscription and Rating of a Service

Finally, Figure 7 presents the interaction needed for the messaging between a user that wants to use a Service and the provider of this specific service.

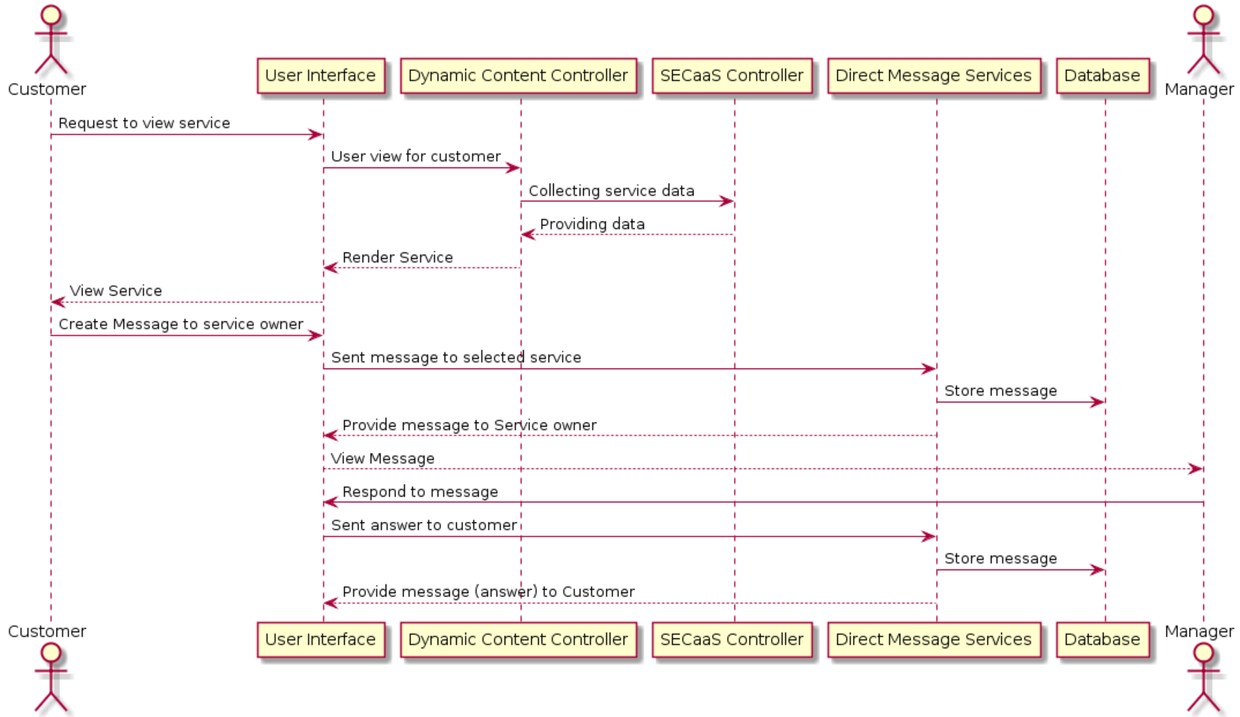

Figure 7: Stakeholder Messaging in the Marketplace

3.1.5 Physical View

The last view of the 4+1 architectural view model is the physical view that depicts the topology of software components on the physical layer as well as the physical connections between these components. Currently, SecureIoT Marketplace has considered an application hosted in a single server, as this is sufficient for the project needs. However, the proposed architecture can be expanded in multiple servers for example with the usage of a separate server for persistent storage and database hosting, or with the separation of the user interface, the controllers and the backend services.

What is important to highlight on this view however is the usage of services that are available on the SecureIoT market. Through the marketplace, SecureIoT provides a central point for accessing services that are offered by partners inside the consortium of SecureIoT and developed during the project, and other services offered by external stakeholders. These services will be installed in separate servers hosted in resources that might not be on the same premises with the SecureIoT marketplace, in many cases in cloud resources. For this reason, it would be beneficial on the services that are offered through SecureIoT to also state the location of the services, as this can affect both the performance (e.g. due to network latency between the user and the service) but also for legal and legislation compliance reasons.

Finally, SecureIoT will provide the SecureIoT services for testing through the exploitation sandbox. Exploitation Sandbox is a set of infrastructure and services that are installed in separate, dedicated resources and is available through SecureIoT marketplace in order to assist the usage of SecureIoT outcomes by the users.

The following Figure 8 depicts the deployment diagram which clarifies aspects of the physical configuration of SecureIoT Marketplace and the related services.

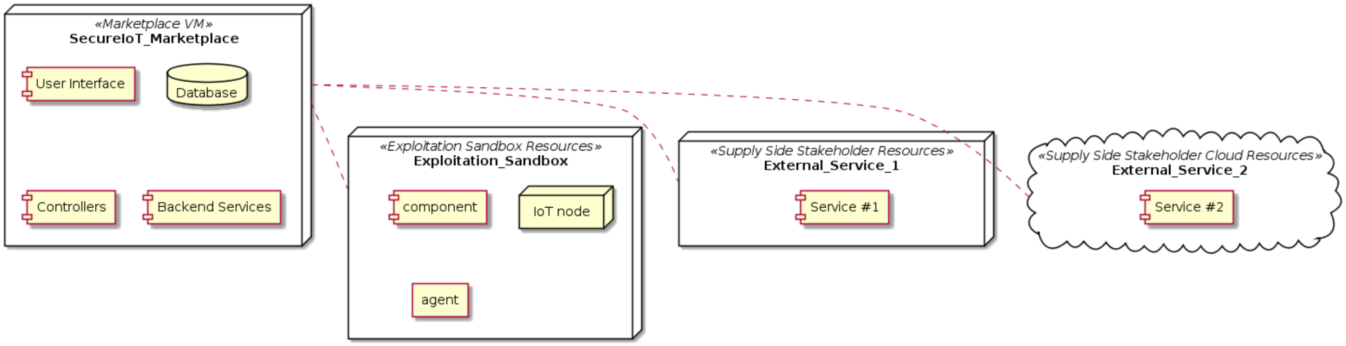

Figure 8: Indicative Deployment Diagram of SecureIoT Marketplace and the offered services

As at the time that this deliverable is written the first version of SecureIoT Marketplace is already deployed and working (marketplace.secureiot.eu), we can provide some details for the current installation. For hosting the marketplace, SingularLogic is using a single Virtual Machine with 2VCPUs and 4GB of RAM, provided by a highly available, privately hosted OpenStack based cloud infrastructure. For this VM, daily backups are performed in order not to lose the marketplace data, always in compliance to the Privacy Policy that will be used by SecureIoT marketplace[2].

3.2 Base Technologies and Technical Solutions for the Implementation of SecureIoT Marketplace

As described in D7.1 we investigated existing open source marketplaces (like Sharetribe[3] or Beyourmarket[4]) that can be used as a base for SecureIoT Marketplace, but create a dedicated platform for this a valid option, due to the high level of customization that will be needed.

In more specific, we implement the marketplace using technologies like Java 8, Spring Framework[5], Spring Boot[6], Thymeleaf[7]() and for storage, MySQL a relational database. This exact stack had been used in the PaaSword project and is also used for the development of Compliance Auditing Service and Programming Support services in WP5, therefore the reuse of the same stack provides additional benefits for the developers of the involved companies (SiLO, UBITECH,

[2] The Privacy Policy of SecureIoT Marketplace is already available on the marketplace: http://marketplace.secureiot.eu/files/SecureIoT%20Marketplace%20-%20Notice%20on%20Personal%20Data%20Processing.pdf

[3] https://www.sharetribe.com/

[4] http://beyourmarket.com/

[5] http://spring.io/

[6] http://spring.io/projects/spring-boot

[7] https://www.thymeleaf.org/

Fujitsu, ATOS) through sharing common practices and code snippets, converging on the website looks, troubleshooting on research issues, etc. More details for the implementation of the marketplace are provided in deliverable D7.7.

3.3 Market Platform Development

The exact status of the marketplace will be presented with more details in deliverable D7.7, however here we provide an overview of the status of the marketplace based on the coverage of the identified specifications at the point that this deliverable is written.

3.3.1 SecureIoT Marketplace Implementation Status

In this section we provide the current implementation status for the Functionalities presented in Table 1. The following table illustrates the status regarding the functionalities' implementation.

Table 3: Platform Functionalities Implementation Status

MSP Ecosystem Functionality	Status / Plan	Comments
Registering Participants & Business Entities	Ready	-
Authentication and Authorization	Ready	-
Search and discovery of service offerings	Not Ready	-
Catalogue Publishing of services	Ready	-
Provision of recommendations	Ready	-
Collaboration Services	Partially implemented	Forum is not available, messaging is available
Review and rating of service offerings	Ready	-
Manage and tracking registered services	Ready	-
Solution Presentation	Ready	-
Services Presentation	Ready	-
Knowledge base	Partially Ready	Publications have been added
Marketplace Layout	Ready	-
Future Monetisation Module (marketplace / e-commerce)	Not Ready	Not planned for the implementation during the project duration
Libraries	Not Ready	-
Developers' support services	Not Ready	-
Training, consulting and technical support services	Partially Ready	Some services are available already, more will be added
Access to Services	Partially Ready	Some services are available already, more will be added
Access to Tools	Partially Ready	Some services are available already, more will be added
Use Case Paradigm	Not Ready	To be done based on WP6 outcomes

Localization	Not Ready	Not planned for the implementation during the project duration
Registration through 3rd party authentication services	Not Ready	-
User and Organization Management	Ready	
Basic Content Management Support	Partially Ready	Some pages are ready

3.3.2 SecureIoT Marketplace Sitemap

As presented in section 2.1.3 the roles created in the marketplace are the following:

- Visitor
- Marketplace Member (Customer)
- Manager
- Moderator
- Administrator

During the development of the marketplace, we tried to extend the mapping of functionalities made on each of these roles in order to provide us with the sitemap that will be provided in the marketplace website.

For the **visitor**, we only provide static content (Knowledge Base, News, Blogs, Project Info), the search function and the login screen.

For the registered members that act as **customers** of the marketplace (demand-side stakeholders) the marketplace website should offer all the static content mentioned for the visitor, the search function, visit forum, view profile and a logout option. Also, the customer can view the available SECaaS Services, SECaaS Business Services and SecureIoT Solutions, and subscribe, rate or contact with a message with the owners of the services.

For the registered members that act as **managers** of the marketplace (supply side stakeholders) the marketplace website should offer all the static content mentioned for the visitor, the search function, visit forum, view profile and a logout option. In addition, a manager can view and edit his/hers SECaaS Services, SECaaS Business Services and SecureIoT Solutions, and reply to messages sent by customers.

The **moderator** is responsible for the management of the platform content; therefore, the moderator can view and edit all the static content mentioned for the visitor, and also view and edit all the SECaaS Services, SECaaS Business Services and SecureIoT Solutions, and any important closed lists assigned to them.

Finally, the **administrator** is provided with user management and organization management page in order to properly manage the users and organizations of the marketplace.

4 Conclusions and Next Steps

In this deliverable, we tried to present how the IoT Security Solutions Market Platform will be built in order to offer a single entry point of interaction for SecureIoT services, documentation, support, etc. The motive for the creation of this marketplaces is to allow easier usage of SecureIoT by stakeholders, the creation of a community of service users and service providers and eventually to give to SecureIoT better sustainability likelihood.

For this purpose, in this document, we presented the work performed in the scope of task T7.1, for the creation of a Multi-Sided Market platform that will offer Security services on IoT based environments. The initial specifications of the Marketplace have been updated and extended in section 2.2 of this document, while the background for building this specification was presented in D7.1. We also identified the roles that the marketplace will offer and how the needed functionalities map to these roles in order to provide some concrete usage scenarios.

These scenarios, along with four different views of the architecture provided use with finer details that will lead to the implementation of the marketplace platform in the scope of WP7. The first version of the marketplace is described in deliverable D7.7

References

[SecureIoTD7.1] SecureIoT D7.1 IoT Security Solutions Market Platform Architecture and Specifications; First version, Angouras George (SiLO) and all, 2018

[SecureIoTD2.4] SecureIoT D2.4 Architecture and Technical Specifications; First version, J. Soldatos and all, 2018.

[SecureIoTD2.5] SecureIoT D2. Architecture and Technical Specifications; Final version, J. Soldatos and all, 2019.

[Kruchten95] Kruchten, "Architectural blueprints - The "4+ 1" view model of software architecture," IEEE Software, 1995.