SecureIoT

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 7.1 - IoT Security Solutions Market Platform Architecture and Specifications_First version

Deliverable Number	**D7.1**
Deliverable Name	**IoT Security Solutions Market Platform Architecture and Specifications_First version**
Dissemination level	Public
Type of Document	Report
Contractual date of delivery	30/09/2018
Deliverable Leader	SiLO
Status & version	1.0
WP / Task responsible	WP7(SiLO) / Task 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:	Angouras George (SiLO)
Contributors:	SiLO, AIT, INTRA
Reviewers:	ATOS, INTRA
Approved by:	George Koutalieris (INTRA)

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.

Executive Summary

The purpose of this document is to describe the rationale and the vision 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 the ability to use SecureIoT through the exploitation sandbox. Additionally, it will also provide relevant technical support, documentation and training capabilities, and will also allow interested stakeholders to publish datasets. 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-Side platform means that there should be the ability to allow service providers to add their services and offer them through SecureIoT Marketplace.

Based on these initial requirements and the analysis of relevant solutions, the specifications and the functionalities that the marketplace shall provide are describe in the document. Based on the specification and the included services on the marketplace, an initial view on the architecture of SecureIoT Marketplace is provided.

The documentation of this task reflects the work done so far in the frames of task T7.1. This first version of the deliverable serves as a starting point for the efforts of WP7 tasks, by identifying specification of the services, based on existing SOTA and also based on the WP5 SECaaS needs. The final version of the IoT Security Solutions Market Platform Architecture and Specifications will be provided in the deliverable D7.2 at M18. At that point, more concrete details about the developed marketplace will be provided, while also liaisons and integration with existing ecosystems will have started.

Document History			
Version	**Date**	**Contributor(s)**	**Description**
v0.1	04/09/2018	Angouras George (SiLO), Tsatsoulas Apostolos (SiLO)	Initial ToC
v0.2	13/09/2018	Angouras George (SiLO), Tsatsoulas Apostolos (SiLO)	1st round input
v0.3	16/09/2018	Angouras George (SiLO), Mardirosian Samuel (SiLO)	2nd round Input and merge of contributions
v0.4	17/09/2018	Angouras George (SiLO), Mardirosian Samuel (SiLO)	Update sections 3.2 and 3.3
v0.5	23/09/2018	Angouras George (SiLO), Mardirosian Samuel (SiLO)	Update sections 4.1 and 4.2
v0.6	24/09/2018	Angouras George (SiLO), Tsatsoulas Apostolos (SiLO)	Ready for review
v0.7	25/09/2018	ATOS, SIEMENS	Review
v0.8	28/09/2018	SiLO, ATOS, SIEMENS	Incorporate version with comments from reviewers
v1.0	30/09/2018	Mariza Konidi (INTRA)	Final version to be submitted

Table of Contents

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

Table of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym	Title
ADC	Application Delivery Control
AIOTI	Alliance for IoT Innovation
BCDR	Business Continuity and Disaster Recovery
CDN	Content Delivery Network
CTI	Cyber Threat Intelligence
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CVSS	Common Vulnerability Scoring System
DL	Deliverable Leader
DLP	Data Loss Prevention
DoA	Description of Action
Dx	Deliverable (where x defines the deliverable identification number e.g. D1.1.1)
EIM	Exploitation Innovation Manager
GSLB	Global Server Load-Balancing
IAM	Identity & Access Management
IoT	Internet of Things
MSP	Multi-Sided Platform
Mx	Month (where x defines a project month e.g. M10)
OrBAC	Organisation-based Access Control
OWASP	Open Web Application Security Project
P-RBAC	Privacy-aware Role Based Access Control
PU	Privacy-aware Role Based Access Control
QA	Quality Assurance
R	Report
RAM	Risk Assessment and Mitigation Service
SEC	Security
SECaaS	Security as a Service
SIEM	Security Information and Event Management
SKB	Security Knowledge Base
SPoC	Single Point of Contact
WAF	Web Application Firewall
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 SECaaS paradigm.

In this context, the purpose of the present deliverable is to describe the IoT Security Solutions Market Platform that will be built in order to offer the aforementioned capabilities to interested stakeholders. Therefore, it will extend SecureIoT outcomes 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 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 and also the installation of an exploitation sandbox that will be part of the marketplace in order to allow the hands-on experience to the users.

Finally, an initial design of the marketplace has been produced, in order to allow the beginning of the development process of the marketplace. As the development will proceed and also the SECaaS will be implemented in the next months, we consider that the architecture is due to changes.

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 platform is still in the design phase, this document has been based mainly in the architectural designs that have been documented in deliverable D2.4 [SecureIoTD2.4].

1.3 Document Structure

The rest of the document is structured in four more sections;

- Section 2 provides a brief analysis of relevant solutions in the fields of IoT platforms and the SECaaS
- Section 3 described the specifications of the marketplace in terms of needed functionalities and also by describing the services that will be offered
- Section 4 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
- Section 5 concludes the document

2 State of the Art and Key Technology Axes Challenges

For the specification, design and implementation of SecureIoT Multi-Sided Market Platform we investigated relevant solutions in the fields of IoT marketplace and the SECaaS market, in order to help on the identification of desired characteristics and specifications for the marketplace to be developed.

2.1 IoT Marketplaces

Software service or software application marketplaces are commonly used for providing discovery, purchase, and distribution of applications and services. Traditional application stores have limitations as far as IoT applications are concerned. Marketplaces for IoT should include authentication, billing, accounting, as well as catalogues for IoT data and applications. To provide a complete solution for IoT users, marketplaces could also be extended with an additional catalogue for communication protocols (platform-specific) and for IoT devices/components [Mineraud16]. Therefore, in order to focus in the IoT field, we examined available IoT platforms that connect smart objects or things to the Internet, in order to assess if and how they provide marketplace characteristics.

Some of the most important IoT Platforms examined are provided in the following table.

Platform	Description
AWS IoT	AWS IoT is a set of services provided by Amazon in order to enable connectivity and management of IoT devices through AWS Cloud Services
https://aws.amazon.com/iot/	
Ericsson IoT-Framework	The Ericsson IoT-Framework is a PaaS that accumulates sensor data from IP networks and focuses on the analytics and the mashing up of the data. The PaaS includes a REST API, data storage functionalities and OpenID access control for the data. The strength of this platform is the publish/subscribe mechanism, and querying of data streams, both from local and external data sources) to perform analytical tasks
https://www.ericsson.com/ourportfolio/iot-solutions/iot-platform	
IFTTT	IFTT is a SaaS offering, allowing a rapid composition of services called “recipes” by applying simple if-then rules to external service building blocks, such as emails, Facebook events, or Belkin’s WeMo switch, that either play the role of a trigger (if) or an action (then, do)[1]. Recipes
https://ifttt.com/	

[1] https://www.mysmartahome.com/if-this-then-that/

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

	can be private or public, thus share with other users.
EvryThng http://www.evrythng.com/	EvryThng is a proprietary centralized platform (SaaS) that provides a persistent presence on the IoT and the Web of identifiable objects (RFID, NFC, connected objects, etc.). It provides a RESTful API to store and retrieve metadata and real-time data for these objects. The API allows fine-access grained control to easy sharing of products information; however, no search tools are available to find data feeds.
DeviceCloud http://www.etherios.com/products/ devicecloud/	DeviceCloud is a cloud-based device management platform that provides access to the devices connected to the platform via a REST API.
Devicehub.net http://www.devicehub.net/	Devicehub.net is a proprietary cloud-based platform which does not provide a true REST API (using GET method to PUT data).
Arkessa http://www.arkessa.com/	Arkessa is a cloud-based management architecture and IoT platform. It includes the MOSAIC platform that enables devices to be easily connected to many applications. Ownership of the data remains to the end-user.
OpenIoT http://openiot.eu/	OpenIoT platform is an open-source platform, fully decentralized, that provides connectivity with constrained devices such as sensors. The platform provides a billing mechanism for the use of services.
Kahvihub http://github.com/uh-cs-iotlab/ kahvihub	The Kahvihub platform is open-source and designed to be extremely extendable, as all components in the Kahvihub are delivered by third-parties, in the form of plugins or applications. The Kahvihub prototype is aiming to enable edge analytics by creating local networks of IoT devices that can collaboratively and autonomously analyse the data that they produce.
ThingWorx https://www.ptc.com/en/products/iot	ThingWorx is a proprietary cloud-based platform (PaaS that provides a variety of connectivity services, software agents and in general tools and services to support end-to-end solutions.
FIWARE	

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

https://www.fiware.org/	FIWARE is an open-source initiative that aims to create a platform to leverage on the combination of disruptive technologies like the *Internet* of Things (IoT), Big Data or Cloud architectures. Rather than proposing a tightly and closed solution that targets the specific requirements of a single domain, FIWARE eases the creation of new applications in multiple verticals since its catalogue contains a rich set of components that can be connected, combine and deploy in a flexible way. FIWARE IoT Agent implementations enable the usage of a wide range of smart objects that go from constrained devices based on microcontrollers to more powerful embedded systems that are to run a complete TCP/IP stack and to apply advanced security features. FIWARE has a centralized marketplace for addons called FIWARE Marketplace (https://marketplace.fiware.org) that serves as a global one-stop shop with main focus the dissemination of existing FIWARE offerings. In that sense, the FIWARE marketplace is one of the main influences for the creation of the specifications, vision and architecture of SecureIoT Marketplace.
TheThingsNetwork https://www.thethingsnetwork.org/	The Things Network is a network for IoT that build on top of abundant data connectivity between devices and applications. It has a dedicated marketplace that hosts IoT-ready products and solutions by third parties. (https://www.thethingsnetwork.org/marketplace)
Azure IoT https://azure.microsoft.com/en-us/overview/iot/	Formerly known as Azure IoT Suite, Azure IoT with its solution accelerators offers customizable IoT templates for common business scenarios. In essence these templates act as the building blocks of an MSP marketplace, as there are available accelerators from Microsoft but also from Microsoft approved partners.
BIG IoT http://big-iot.eu/	BIG IoT is a Horizon 2020 funded project that has the vision to create cross- standard, cross-platform, and cross-domain IoT applications. Among the goals of BIG IoT is to create a marketplace for the advertisement, discovery,

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

	monetization, and reuse of applications by the ecosystem participants.
Siemens MindSphere	MindSphere represents one of the largest industrial initiatives in the area of Internet of Things worldwide. MindSphere is designed in a loosely coupled manner, micro-service oriented, allowing natural scalability of customer needs. It is structured to provide customers both scalability at the level of gateways towards the shop floor (managed via MindConnect) and at the end of data analytics users willing to extract meaningful insights, where it exposes REST APIs. MindSphere expose a set of continuously evolving services platform structured around relevant usage scenarios for the whole platform. From a security point of view MindSphere use for MindConnet Library a secured connection using SSL/TLS aiming to protect customer data, and a dedicated IAM framework (Identity & Access Management)
CloudCare2U	CloudCare2U is iSprint's IoT platform focuses on the practical issues with regards to security and privacy, such as the security management and the overhead and scalability of the access control by introducing novel solutions based on concepts like CP-ABE, Single Point of Contact (SPoC), Organisation-based Access Control (OrBAC), Privacy-aware Role Based Access Control (P-RBAC), Trust negotiation-based access control, etc.

Table 1: Relevant IoT Platforms

Our focus was to investigate the marketplace characteristics on the IoT platforms. Among the plethora of IoT platforms only a few have marketplaces that provide services (e.g. ThingWorx, IFTTT, Azure, TheThingsNetwork) and only some (OpenIoT) promise to enable the (usage-based) charging of the end users of these applications [Mineraud16].

Some platforms also allow the sharing of data. One of the key challenges of IoT is to exploit all the data that is currently being produced by businesses. According to McKinsey[mckinsey], businesses already collect a tremendous volume of sensor data but the data is only used for anomaly detection and control. However, data should also be used for optimization and prediction which provide the greater value, but businesses may lack the expertise to analyse and process their data. SecureIoT can be a driver towards this direction, as it can provide an IoT platform that has a marketplace that allows businesses to publish data streams to the platform

in order to make them available through a browsable catalogue to a large number of application developers.

A marketplace that acts as an extension to an IoT platform shall offer information about pricing or even better to provide the possibility of charging for the data consumption either by a time-defined subscription or by the amount of data to be consumed. Of course, publishing data streams free of charge can be a good way to disseminate and gain the critical mass of stakeholders. Therefore, an IOT marketplace should include authentication, billing, accounting, as well as catalogues for IoT data and applications.

An overview of a typical IoT marketplace is provided in Figure 1 below.

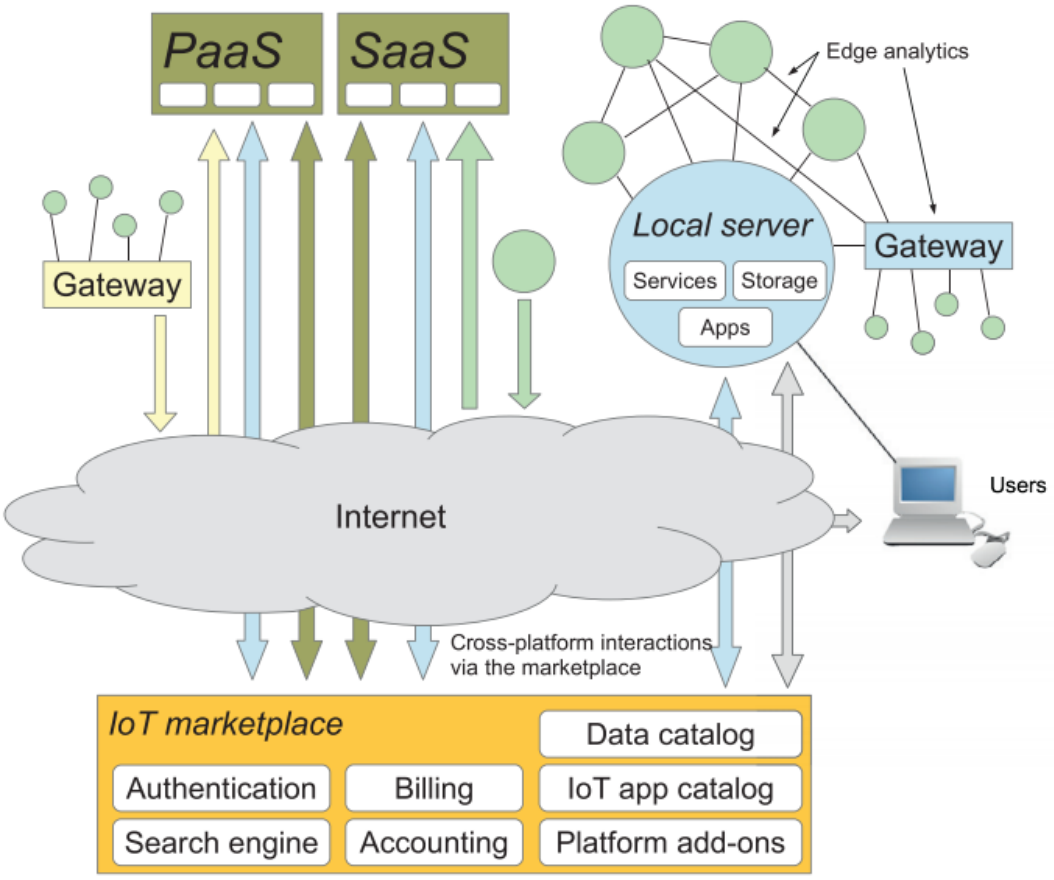

Figure 1: Interactions of an IoT Marketplace and IoT platforms according to J. Mineraud et al (source : [Mineraud16])

Both the internal artefacts and the deployment characteristics of the presented schema have been taken under account for the design of the marketplace as presented in section 4.

One of the fundamental criteria for IoT platforms is the need to include efficient and reliable privacy and security mechanisms. Satyadevan et al. surveyed IoT platforms with respect to security and trust management. The survey suggests that cloud-based IoT platforms are prone to

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

traditional web and network security attacks such as Denial of Service (DoS), man-in-the-middle, eavesdropping, spoofing and controlling attacks [Satyadevan]. However similar seems to be the cases regarding the security and privacy also in both centralized and distributed IoT scenarios [Roman13]. Therefore, there is a number of areas that security can be provided in the IoT platforms and Secure IoT marketplace through the provided SECaaS can help towards this direction.

2.2 Security as a Service (SECaaS) and SECaaS Marketplaces

As the existing IoT platforms, and especially marketplaces don't have embedded the offering of security services, we also investigated platforms that provide concrete security services through the SECaaS paradigm, in order to define the characteristics and the specifications of SecureIoT marketplace.

Some of the most important platforms offering SECaaS are examined are provided in the following table.

Platform	Description
Incapsula	Incapsula WAF provides solutions to protect websites against SQL injections, cross site scripting, illegal resource access and all other OWASP[2] top 10 threats, and web 2.0 threats including comment spam, referrer spam, fake registrations, site scraping, malicious bots, and academic web archiving. Incapsula has different features that are used in the security and performance of websites: • Web Application Firewall (WAF) • DDoS Mitigation • Application Delivery Control (ADC) • Global Server Load-Balancing (GSLB) • Content Delivery Network (CDN)
CloudFlare	Cloudflare is a platform that provides as a service DDoS protection and WAF. Also provides Authoritative DNS and a Public DNS resolver, reverse proxy and a content delivery network (CDN)
CloudFabric	CloudFabric is a platform that provides WAF and can protect from SQL injection, cross-site scripting, identity theft, website defacement, and application layer DDoS attacks
Azure Security as a Service	

[2] https://www.owasp.org/index.php/Main_Page

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

https://www.microsoft.com/en-us/CloudandHosting/SECAAS.aspx	Azure Security as a Service is a dedicated platform of Microsoft for allowing the easy securing devices, apps, data, and identities that use Azure Cloud.
AIONCLOUD https://www.aioncloud.com	AIONCLOUD provides Cloud WAF and a web security service that provides malware detection based on diagnosis, in order to boost website performance, secure websites and minimize security risk.
Zscaler https://www.zscaler.com/products/cloud-architecture-security-as-a-service	Zscaler is a security as a service is provided through distributed data centers over the world in order to provide optimal performance. Among others, it provides WAF, DNS and URL Filtering, DNS Security and Cloud Sandbox.
Fortinet https://www.fortinet.com/solutions.html	Fortinet provides managed security service platofrm that offers WAF, SIEM, Sanboxing as a service. Fortinet also provides IoT related solutions but not as part of the managed security service.

Table 2: Relevant SECaaS Platforms

It has to be stated that the aforementioned platforms are not suited for security over IoT environments, with the exception of Fortinet that has IoT security solution but cannot be provided through their managed security platform. In general, for the delivery of SECaaS a security knowledge base is required in order to store knowledge collected and summarized based on multiple publicly available threat intelligence sources. This data combined with the metadata of IoT entities should allow the enforcement of security capabilities.

SECaaS paradigm, does not imply that the security services are solely deployed in the cloud. Rather, they can be offered based on a combination of cloubased SaaS (Software-as-a-Service) security services and FaaS (Fog-as-a-Service) functions provided at the fog level. In SecureIoT the decision on how to provide the SECaaS is still pending, but will probably depending on each specific SECaaS.

Apart from the differentiation about the placement of the SECaaS, pricing is another point that has to be taken under consideration for the building of the marketplace, with SECaaS typically offered in Subscription based approach, with Payment for utilized services or even free of charge (e.g. AIONCLOUD, Cloudbric, CloudFlare, and Incapsula)

Finally based on Cloud Security Alliance (CSA)[3] the following categories of SECaaS have been identified [CSA2016].

[3] https://cloudsecurityalliance.org/group/security-as-a-service/#_overview

- Business Continuity and Disaster Recovery (BCDR or BC/DR)
- Continuous Monitoring
- Data Loss Prevention (DLP)
- Email Security
- Encryption
- Identity and Access Management (IAM)
- Intrusion Management
- Network Security
- Security Assessment
- Security Information and Event Management (SIEM)
- Vulnerability Scanning
- Web Security

For SecureIoT the identified categories will be used for the categorization of the SECaaS in the created marketplace.

3 Market Platform Specifications

3.1 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
- systematic access to business / technical support and consulting,
- detailed exhibits of hands-on use-cases (WP6),

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

3.1.1 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

3.1.2 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.

3.1.3 Benefits that SecureIoT Multi-Sided Platform provides

3.1.3.1 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.

3.1.3.2 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.

3.2 Specifications of Core Market Platform Features

The following table illustrates some of the core functionalities and features that the ecosystem should include

MSP Ecosystem Functionality	Short Description
Registering Participants & Business Entities	Registration of participants to the ecosystem
Authentication and Authorization	Ensuring authenticated and authorized access to the various services and sections of the platform
Search and discovery of service offerings	Search engine for discovering available services based on appropriate metadata for the services descriptions

Catalogue Publishing of services	Publication and presentation of the ecosystem services, solutions, tools, and other entities described in WP2
Provision of recommendations	Context-aware proposition of relative service offerings
Collaboration Services	Collaboration Services (e.g., Forum/Messaging/Repository), including the relevant community support
Review and rating of service offerings	Tools for rating service offerings from the end-users / participants viewpoints
Manage and tracking registered services	Access to the status of subscriptions and services
Solution Presentation	Solution presentation through examples
Services Presentation	A comprehensive list of all services described in WP6
Knowledge base	Information Services including articles, presentations, News, Blog etc. On-line training and education services in the form of self-contained presentations
Marketplace Layout	Aggregation of Services and Solutions in categories/subcategories with searchable metadata, thumbnails, descriptions, ratings. Content Management features for addition/deletion/categorisation etc.
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
Libraries	Middleware libraries for SEC, SECaaS and general IoT, as well as open APIs for accessing the libraries including accompanying documentation
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
Training, consulting and technical support services	These services will be offered in the form of complementary (augmented) added value 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)
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)
Use Case Paradigm	End to end implemented solutions serving as an example of integration: (smart manufacturing -Industrie 4.0, connected cars and IoT-enabled socially assistive robots)
Localization	Support for an international environment through appropriate localization of the services including currency and language support

Table 3: Platform Functionalities

3.3 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:

3.3.1 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.

3.3.2 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, a new CSA (Coordination and Support Action), titled IoT4EU will commence during the last quarter of 2018 in order to coordinate the activities of these projects. SecureIoT will share and exchanges 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.

3.3.3 IoT-EPI (European Platforms Interoperability)

SecureIoT will establish close links with the IoT-EPI initiative, which includes several IoT platform with different functionalities, capabilities and target application areas. These platforms can provide inputs (e.g., data, services) to the exploitation sandbox of the SecureIoT market platform. Likewise, their development teams are likely to have an interested in the SecureIoT results and the SecureIoT market platform (including its content and services). Moreover, given that IoT-EPI is focused on the issue of interoperability across different platforms it can serve as a basis for demonstrating the security interoperability features of SecureIoT.

3.3.4 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).

3.3.5 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
- 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

3.3.6 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.

3.4 Component and Services Offerings

Here we can have the list of services or components that we will offer, but also others like technical support services, integration services, training services, business support services etc.

3.4.1 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 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.4.5 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.

3.5 Additional Services

In addition to the services offered by the platform (mostly SECaaS but also third-party services if possible), the following services will be part of the marketplace in order to assist on the adoption of SecureIoT from users and making the SecureIoT ecosystem a more complete solution.

3.5.1 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.

3.5.2 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.

3.5.3 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.

4 Market Platform Architecture

In this section we present the architecture of SecureIoT Market Platform. The vision of SecureIoT is to implement an 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 data their data to the SecureIoT services provider i.e. the entity that is deploying and operating the SecureIoT platform. This approach covers the 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).

4.1 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. 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. The present deliverable has put emphasis on the presentation and elaboration of the logical view, as the most important view of the system, while in deliverable D7.2 the other views of the architecture will be provided. In the following figure the conceptual architecture of SecureIoT Marketplace is provided.

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

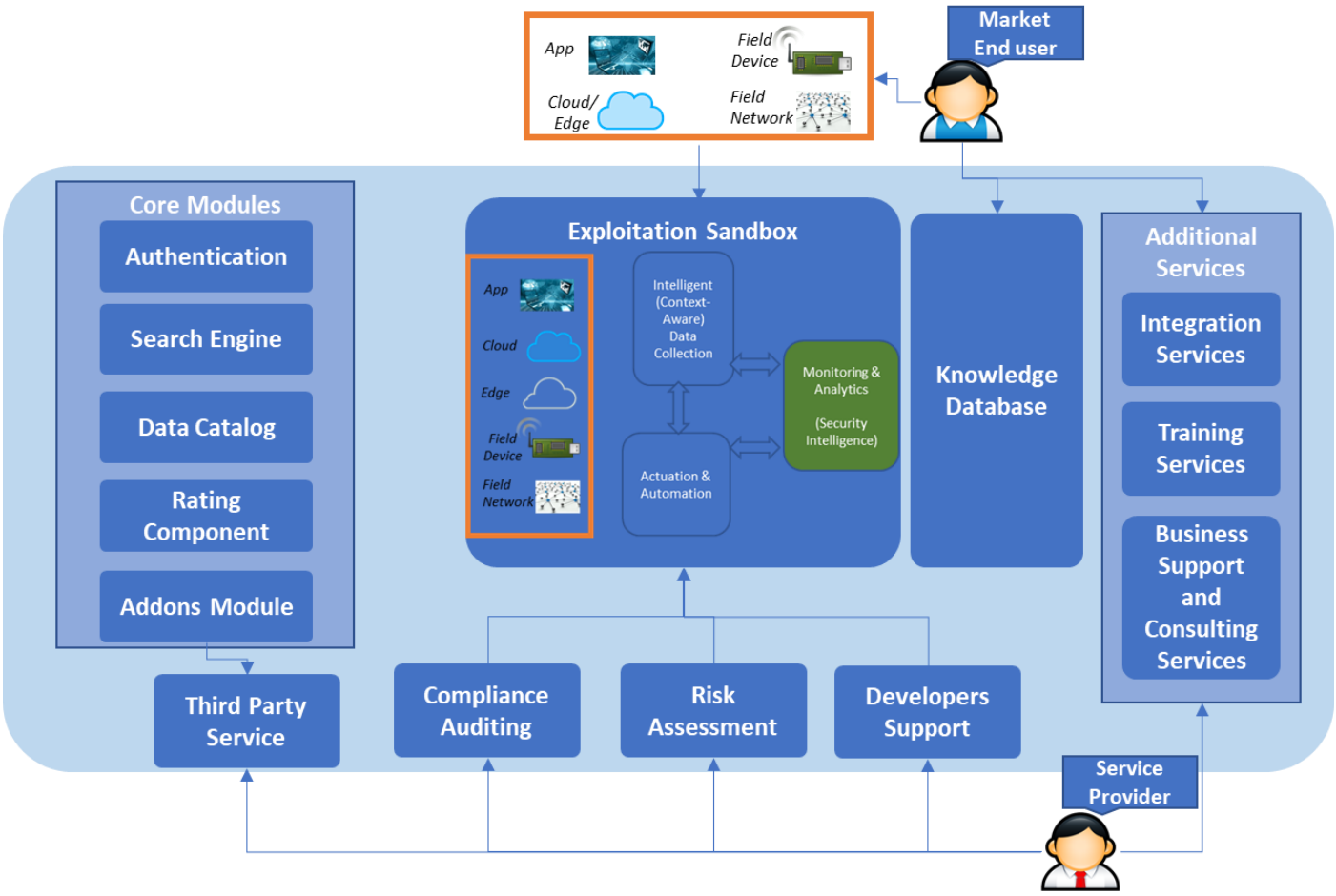

Figure 2: High Level Logical View of the SecureIoT Marketplace

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. 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 offer 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) though 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

Project Title: SecureIoT
Contract No. 779899
Project Coordinator: INTRASOFT International S.A.

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.

- **Third Party Services:** This includes services that can be added by third parties by are connected to the SecureIoT platform (and the SecureIoT marketplace through the Addons module)

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

Although there is a number of existing open source marketplaces(like Sharetribe[4] or Beyourmarket[5]) that can be used as a base for SecureIoT Marketplace, we consider the possibility to create a dedicated platform for this a valid option, due to the high level of customization that will be needed. Therefore, we shall implement a solution using technologies like Java 8, Spring Framework[6], Spring Boot[7], Thymeleaf[8]. For storage, a relational database like MySQL can be used.

[4] https://www.sharetribe.com/
[5] http://beyourmarket.com/
[6] http://spring.io/
[7] http://spring.io/projects/spring-boot
[8] https://www.thymeleaf.org/

5 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 into the analysis of the characteristics needed for the creation of a Multi-Sided Market platform that will offer Security services on IoT based environments. The specifications of the Marketplace have been identified and described in the document and an initial design of the marketplace has been produced.

In the following months, the created architecture will be used for the implementation of the marketplace, while as other WP7 tasks will start, the designed platform might be extended based on the efforts regarding liaisons and integration with existing ecosystems, and the integration with third-party security & privacy solutions. The advances in the frames of task T6.1 and the design of the SecureIoT Marketplace will be delivered in the final version of this document, in deliverable D6.2 (IoT Security Solutions Market Platform Architecture and Specifications_Final version) that is due on M18.

References

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

[Mineraud16] J. Mineraud et al., A gap analysis of Internet-of-Things platforms, Computer Communications (2016),http://dx.doi.org/10.1016/j.comcom.2016.03.015

[Satyadevan] S. Satyadevan, B. Kalarickal, M. Jinesh, Security, trust and implementa- tion limitations of prominent IoT platforms, in: S.C. Satapathy, B.N. Biswal, S.K. Udgata, J.K. Mandal (Eds.), Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Volume 328 of Advances in Intelligent Systems and Computing, Springer Inter- national Publishing, 2015, pp. 85–95, doi: 10.1007/978- 3- 319- 12012- 6 _ 10 .

[Roman13] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279. (Towards a Science of Cyber Security and Identity Architecture for the Future Internet) http://dx.doi.org/10.1016/j.comnet.2012.12.018 .

[CSA2016] Defined Categories of Security as a Service. Available online at: https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf

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