EUSEC

EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D7.2 INNOVATION MANAGEMENT PLAN

VERSION 1.1

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: June 30, .2017	DELIVERY DATE: December 19, 2018
AUTHOR: Linda Strick, Alexander Mappes (Fraunhofer)	PARTNERS CONTRIBUTED: Alain Pannetrat, Christian Banse
DISSEMINATION LEVEL:* PU	NATURE OF THE DELIVERABLE:** R
INTERNAL REVIEWERS: NIXU, Caixa	
*PU = Public, CO = Confidential	**R = Report, P = Prototype, D = Demonstrator, O = Other

This project has received funding from
the European Union’s HORIZON Framework
Program for research, technological development and
demonstration under grant agreement no 731845

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	20/08/2018	Initial version	Alexander Mappes, Fraunhofer
1.1	15/12/2018	Split from combined Deliverable D1.1/D7.2, added with Business Model Canvas Approach	Alexander Mappes, Fraunhofer

EXECUTIVE SUMMARY

In the following a description of the Innovation Management Plan is given. This includes activities regarding the preparation for the exploitation of the innovations developed during the EU-SEC project.

First, existing tools and technologies implemented in the project are systematically evaluated, based on the TRA methodology (outlined in D1.1). When the evaluation took place, two of the assessed tools were rated with a TRL < 7. Therefor for these two tools specific activities are outlined, that aim at improving the technological maturity of these tools.

Hereafter, two newly generated approaches are described as a combination of existing tools, which make up the major innovations of the project, that are eligible for further exploitation. The Continuous Auditing based Certification, on the one hand, represents a semi-automated auditing process for cloud security standards. The Multi Party Recognition Framework on the other hand stands for a process innovation defining the principles, criteria, processes and technical capabilities for the mutual recognition between various national, international and sector specific cloud security certifications and attestations.

Finally, methods are outlined, which will be used for the realization of the exploitation of these two innovations. The applied methods include the Value Proposition Canvas [1] and the Business Model Canvas [2] by Alexander Osterwalder. Despite the description of these methods, the procedure of implementing them will be given.

Disclaimer: The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

ABBREVIATIONS

MRL — Market Readiness Level: A theoretical construct / measure describing the effort made, to exploit a technology economically.

TRL — Technology Readiness Level: A theoretical construct / measure used to make the maturity of a technology comprehensible and comparable to other technologies.

TRA — Technology Readiness Assessment: The process of assigning a specific TRL to a technology.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

The aim of the Innovation Management Plan is the definition of further activities towards the development of innovations within the EU-SEC project. This includes the acceleration of the technological maturity of single tools involved in the project. Therefore, the TRLs of the single tools involved in the EU-SEC project will be defined in the chapter Technology Readiness Assessment of Existing Tools. Hereafter, next steps for the further development of these tools are listed in the chapter Action Plan – Further Development of Existing Tools.

Furthermore, the Innovation Management Plan aims at defining new innovations, which can be seen as a combination of existing tools, new processes or the generation of innovative applications for these. The two most promising innovations will be described in the chapter Resulting Innovations. As an innovation is not only defined by its technological newness but also by its market acceptance [3], the creation of new innovations should always concern the demands and needs of potential customers and should therefore implement them in the ongoing developmental process. For this reason, in the EU-SEC project methods are used, that take both customers' and developers' points of views into account. The chapter Innovation Activities Concerning Exploitation introduces these methods. The first method used is the Value Proposition Canvas [1] which is implemented in order to involve potential customers (represented by the project partners Caixa Bank, Fabasoft, NIXU, SixSq, Ministry of Finance of the Slovak Republic and Ministry of Public Administration of the Republic of Slovenia) in the ongoing development. This approach includes the definition of the core features and functionalities of the innovations by clarifying the most significant customer needs and pains [1]. As a result, the activities derived from the Innovation Management Plan can be described as validated by actual customers and should therefore be close to the actual market demand. The second method used is the Business Model Canvas by Alexander Osterwalder [2]. The aim of this method is the generation of potential business models for the most promising innovations derived from the EU-SEC project. The method represents a lean but structured approach, which is based on the predefined value propositions of the single innovations. The potential business models are created by defining potential markets, describing customers segments, customer relationships, distribution channels and revenue streams. After describing the implemented methods, the procedure of how these methods are used within the EU-SEC framework will be outlined in the chapter Procedure.

2 TECHNOLOGY READINESS ASSESSMENT OF EXISTING TOOLS

In order to provide a standardized process promoting the maturity level of each component of the EU-SEC framework, a guided innovation plan will be outlined in the following. This is done to subdivide the rather complicated and entangled process of innovation management into single, clear-cut steps, which can be monitored and maintained successively with ease.

Before activities concerning the promotion of a technology's exploitation are conducted, a detailed definition of the TRL of the implemented tools has to take place. According to the TRA methodology outlined in EU-SEC Deliverable D1.1 [10] this is accomplished by defining the description, the requirements, the verification, the viability and the MRL of the technology. After the current TRL is assessed systematically, KPIs need to be defined, which the technology has to fulfill in order to reach the next TRL. In line with the TRA methodology, the KPIs should as well be classified into the technology's description, requirements, verification, viability and MRL. From these KPIs specific activities can be derived in the next step which are then implemented during the subsequent laboratory or real environment test run. These activities should be consolidated into checklists, tables, graphs or questionnaires to provide a structured and standardized monitoring process during the impending test run. After the test run is finished, the fulfillment of the previously defined KPIs needs to be evaluated: a positive evaluation results in the technology's assignment to an advanced TRL, a negative evaluation makes a recapitulation of the defined KPIs and the associated actions as well as a re-test obligatory.

The following figure shows the key components and procedure implemented during the suggested iterative innovation management plan for the EU-SEC project.

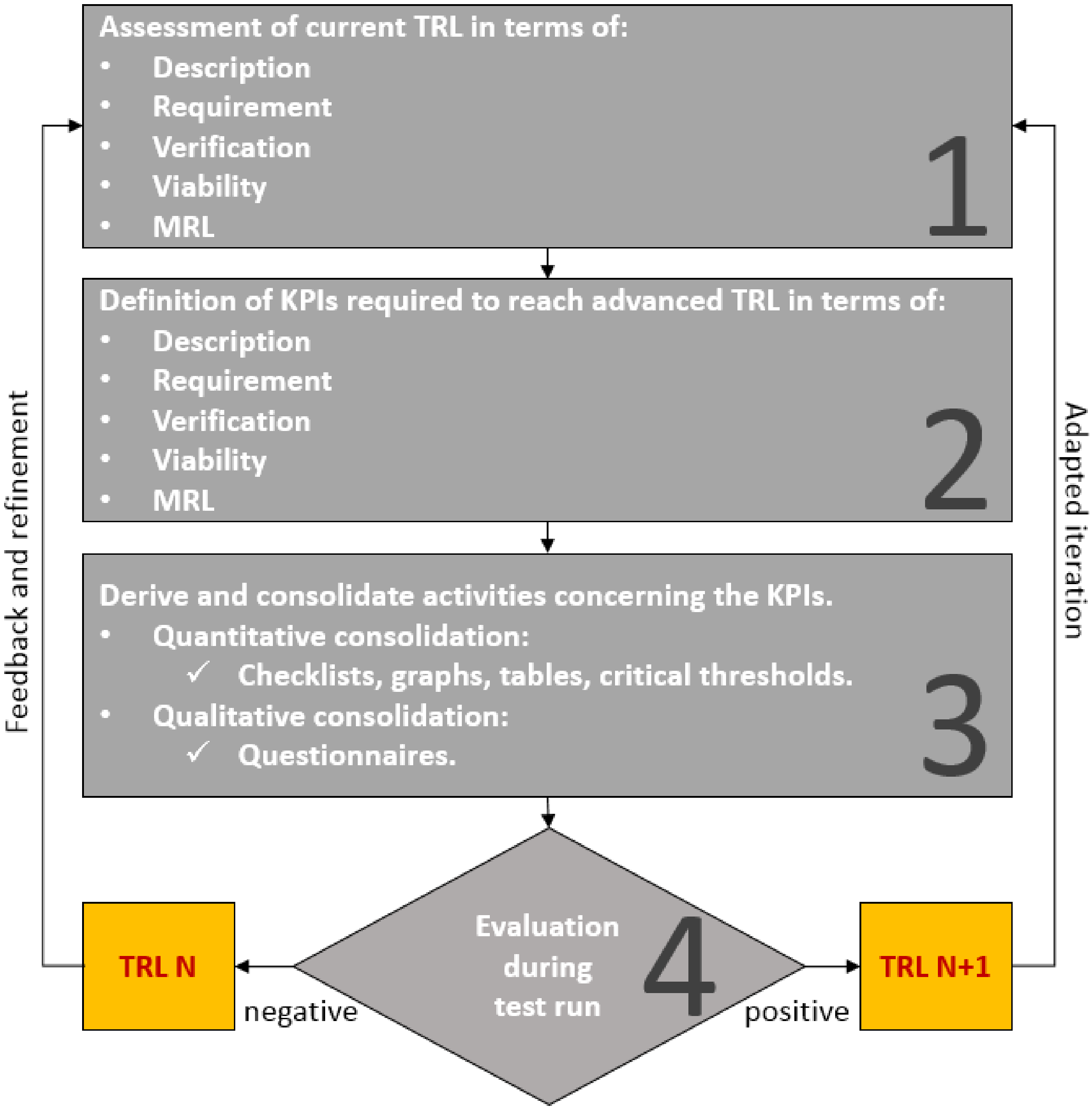

Assessment of current TRL in terms of:
Description
Requirement
Verification
Viability
MRL
1
Definition of KPIs required to reach advanced TRL in terms of:
Description
Requirement
Verification
Viability
MRL
2
Derive and consolidate activities concerning the KPIs.
Quantitative consolidation:
Checklists, graphs, tables, critical thresholds.
Qualitative consolidation:
Questionnaires.
3
Evaluation during test run
4
negative
positive
TRL N
TRL N+1
Feedback and refinement
Adapted iteration

Figure 1: Iterative Innovation Management Plan

This iterative process of assessing the current TRL (1), deriving advanced KPIs (2) as well as associated actions (3) and evaluating the fulfillment of these KPIs (4) is repeated until the intended innovation aim of a TRL 7+ is reached for each component of the EU-SEC framework. In the context of the EU-SEC project, this process implies that for each single component a KPI assessment or evaluation respectively has to take place before, during and after each pilot phase.

This section analyzes the TRL of the tools, techniques and methods making up the EU-SEC framework. The assessment of the TRL of each component will follow the TRA guidelines outlined in EU-SEC Deliverable D1.1. So, for each EU-SEC component with a TRL < 7 a general description of the technology will be provided first, followed by detailed information concerning the description, the requirement, the verification, the validity and the MRL of the technology specifically. This is done in order to establish a systematic, coherent and objective framework for assessing the state of development of each EU-SEC component. According to the specific criteria or KPIs defining an EU-SEC component's actual TRL, we will further derive explicit actions needed to be taken in order promote further development of the individual component. The individualized innovation plans derived hereby and defined for each individual component in the following will be implemented subsequently during the EC-SEC project.

The following table provides an overview of all the EU-SEC components, with those highlighted which are currently assigned a TRL < 7 and are therefore part of the outlined innovation plan.

Table 1 TRL of components of the EU-SEC framework

Existing tools/techniques/methods to be brought	**Owning partner**	**Description**	**TRL**
STARWatch	CSA	CSA STARWatch [4] is a web-based Cloud GRC management tool developed to help organizations to manage the creation and implementation of their enterprise-wide cloud security policies.	9
Open Certification Framework (OCF) / STAR Program	CSA	OCF – STAR Program is CSA's standard for security certification. OCF is organized in three different levels, each one providing different degrees of assurance associated to the Cloud Service Provider.	9
Nuvla / SlipStream	SixSq	SlipStream is an open source multi-cloud application deployment engine. Nuvla is the online managed service broker, based on SlipStream.	9

C5 - Cloud Computing Compliance Controls Catalogue **(Anforderungskatalog)**	PwC Germany / BSI	German BSI released a Cloud Compliance Control Catalogue (C5) that describes a baseline of security measures for a Cloud Service Provider. The security measures are aligned with general accepted standards for information security (e.g. ISO/IEC 27001, AICPA Trust Service Principles and Criteria).	8
Halo	PwC Germany	Halo is a tool that can be used to analyse large volumes of transactions. The built-in algorithms and visualizations help the auditor to understand the client's businesses and assess risk more efficiently. This enables the auditor to focus on items of significance to the audit.	9
Cloud Control Matrix (CCM)	CSA	CCM is a cloud relevant information assurance control framework. Provides standardized security and operational risk management. Provides organisations with structure/clarity relating to information security tailored to the cloud industry. Strengthens existing information security control environments by emphasizing business information security control requirements.	9
Cloud Trust Protocol (CTP)	CSA	CTP complements traditional audits with continuous monitoring. It should be noted that CTP does not define a monitoring technology, but rather a specification for one important aspect of a continuous monitoring technology.	4
Clouditor	Fraunhofer AISEC	Fraunhofer AISEC is developing a prototype called Clouditor (Project NGCert) which supports continuous, test-based audits of security as well as quality of service requirements. Clouditor provides a plug-in architecture which leverages existing security testing tools to support audit of various cloud service models.	4
Fabasoft Cloud	Fabasoft	The Fabasoft Cloud is a Software-as-a-Service solution that lets	9

		organizations digitize their internal and external business processes, the know-how of a customer's employees as well as business documents in agile cooperation with partners and customers. This ensures that know-how is used effectively within the company and on mobile devices while it remains protected.	

2.1 CLOUD TRUST PROTOCOL (CTP) SERVER

Formally speaking, CTP is a specification for a RESTful API that allows cloud providers to report information related to the security of their information system to cloud consumers. The CTP API notably defines how to present SLOs (Service Level Objectives) and measurement results in JSON. To test the validity of the CTP API specification and showcase the concepts behind CTP to the community, CSA created a prototype implementation that implements this API: **the CTP server**.

The following diagrams provide a general idea of the principles of CTP through 3 simple use cases where a cloud service customer uses CTP to query a cloud service provider about security attributes of its services. In the first figure (**A**), the cloud service customer uses CTP to query a cloud service provider about the service availability level that it is committed to provide. In CTP the result of this query is called an "objective" — or "service level objective" — since it describes what the provider aims to achieve, as typically described in an SLA.

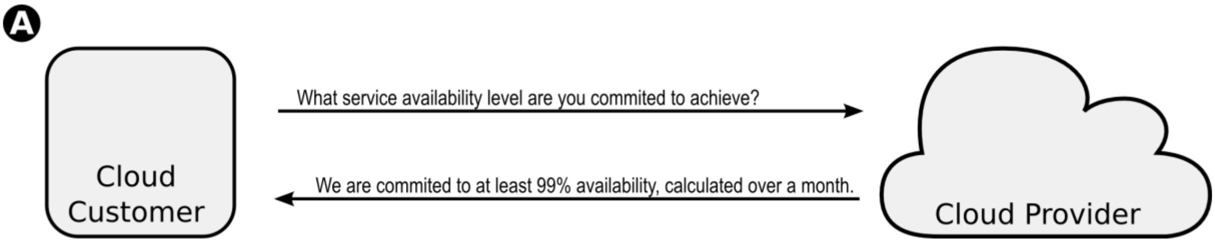

A
Cloud Customer
What service availability level are you commited to achieve?
We are commited to at least 99% availability, calculated over a month.
Cloud Provider

Figure 2: CTP used to query a CSP about the service availability level

Next, in figure (**B**), the cloud service customer queries the cloud provider about the service availability level that was actually achieved in the past month. The result of this query is called a "measurement result" in CTP, since it describes the result of a service level measurement reported by the cloud provider. Both this measurement result and the objective in the previous example apply to the same security attribute informally called "availability" here.

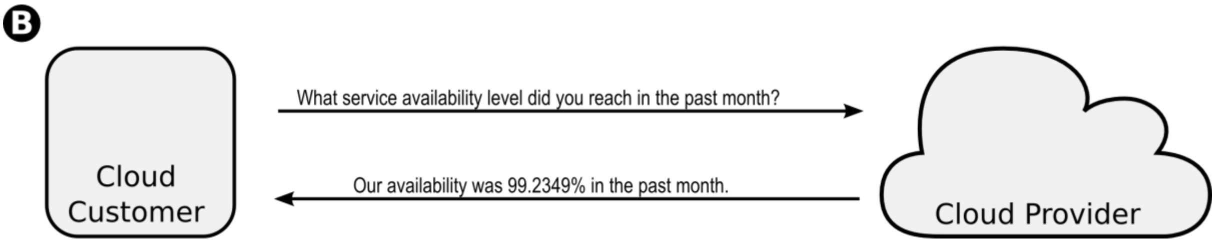

B
Cloud Customer
What service availability level did you reach in the past month?
Our availability was 99.2349% in the past month.
Cloud Provider

Figure 3: Cloud service customer queries the cloud provider about the service availability level

Finally, in figure (**C**), the cloud service customer asks the cloud provider to send an alert when a specific condition is verified. This is called a "trigger" in CTP. In addition, the cloud provider will also log the details of this alert locally for future consultation by the customer.

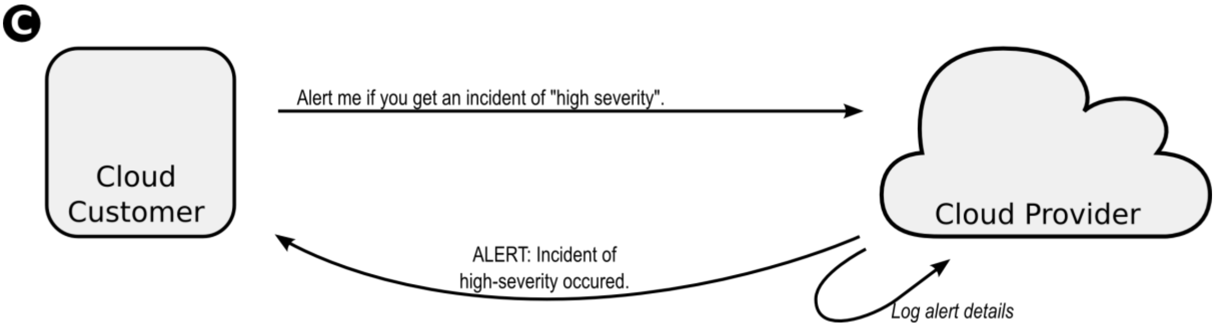

C
Cloud Customer
Alert me if you get an incident of "high severity".
Cloud Provider
ALERT: Incident of high-severity occured.
Log alert details

Figure 4: Cloud service customer asks the cloud provider to send an alert

Naturally, for simplicity, these examples leave out a lot of details that addressed in the specification.

Description:

The CTP server is a standalone application designed to run on Unix-style operating systems. The application is written in Go and uses a MongoDB database backend. For testing purposes, the server offers also an optional lightweight JavaScript client that cloud customers can use to query the CTP server.

The CTP server implements the CTP API defined the CTP Data Model and API [5] and extends it with a non-official "back-office" REST API [6]. While the CTP API is designed to manage standardized interactions between cloud customers and cloud providers, the "back-office" API is designed to allow the cloud provider to easily update the data that is stored by the CTP server and provided to the cloud customer. This approach makes the CTP server more platform-independent since all interactions of the CTP server are implemented through RESTful APIs.

Requirement: The required functionalities of the CTP Server are fully documented in the CTP Data Model and API [5] and the "back-office" REST API [6]. Almost all functionalities of the specification have been implemented:

Currently implemented functionalities:

- Ability to query a cloud provider about the security level of a cloud service.
- Ability to query a cloud provider about security level objectives.
- The ability to define alerts (i.e. "triggers").
- Ability for the cloud provider to create, update and delete data related to the security level of a cloud system.
- Tag based-access control.

Missing or incomplete functionalities:

- Notifications of cloud customers through XMPP messaging.
- The ability to represent relationship between several cloud services.

Verification: The CTP server is used in a demo simulating a Cloud Service Povider, which offers https-secured blogs to its customers, with two SLOs: one for availability and one for cryptographic strength in SSL/TLS. The demo is based on Docker technology, allowing to simulate multiple customers running real instances of a secure blog service.

A video showcasing the demo is available here:

https://www.youtube.com/watch?v=afm4xIEOKqQ&t=32s

CTP has also showcased in the EU funded research project SPECS.

Viability:

While the CTP Server is based on a scalable foundation (Go and MongoDB), as a proof of concept, it has not been fully engineered and tested yet for scenarios where thousands of tenants are using the service simultaneously. The opportunity to test the CTP Server in such a setting would require involvement by a cloud provider.

MRL: The real challenge to CTP is industry adoption: the CTP server is only here as a demonstration tool, not a final product. We need to see the CTP API adopted by a big player (e.g. RackSpace, Amazon, Google), or integrated in a leading open-source cloud (e.g. OpenStack).

We have an active workgroup with industry stakeholders and have presented CTP at industry oriented events. We can summarize what we have learned from these interactions:

- Cloud customers would strongly welcome CTP, especially those with strong regulatory requirements towards continuous monitoring: financial institutions and health sector.
- Major cloud providers are still reluctant to adopt CTP and the level of transparency that comes with it.
- There is still significant work ahead with industry stakeholders in order to define common metrics for security and privacy in the cloud, which is needed to make CTP useful.

Conclusion: CTP is regarded as TRL4.

2.2 CLOUDITOR

Fraunhofer AISEC is developing a prototype called Clouditor, originated from the funded research project NGCert, which supports continuous, test-based audits of security as well as quality of service requirements. Clouditor provides a plug-in architecture which leverages existing security testing tools to support audit of various cloud service models.

Description:

The Clouditor is designed with a micro-service approach in mind and consists of several main modules as well as a plug-in architecture to support the addition of supplementary test definitions, tools and metrics.

- The Clouditor Engine continuously executes a defined set of tests to check whether a cloud service complies with a set of requirements and reports its results.
- The Clouditor Simulator and Evaluator components are responsible for calibrating the test and metric functions. They can be used to simulate the violation of a metric and detection, respectively. This allows for a fine-grained calibration of the metric and test tools.
- The Clouditor Explorer is responsible for defining necessary test parameters of the audited cloud services, such as IP addresses, URLs or desired metrics. This component is in early stages of the development. Fraunhofer AISEC is currently in the process of

designing appropriate interfaces to other Clouditor components as well as other cloud services and first implementation steps have begun.

- The Clouditor Dashboard serves as a management console as well as an overview of the results gathered by other components

Requirement:

All modules have defined interfaces between them, either in the form of an API or a shared database scheme. Each module can be deployed independently from each other as long as API or database access is allowed between deployments. To support this, Fraunhofer AISEC is heavily using container technologies, such as Docker. Thus, all modules are available as pre-built Docker images.

Verification:

The Clouditor is developed within a Continuous Integration (CI) workflow at Fraunhofer AISEC. Source code is maintained at a central git repository, following the git flow model [7]. All changes to the git repository automatically trigger a build process in a Jenkins CI server. The build is executed according to a pre-defined Jenkinsfile which compiles the Java source code and runs individual unit as well as integration tests. While unit tests are designed to test individual functions or functionality within one module, the integration tests observe the behavior of the modules with an embedded test infrastructure (also based on Docker containers). The last step of the build is a code quality check using the tool SonarQube. Only if all the previous steps are executed correctly, the build is passed. Once a build is passed, it is automatically deployed into two test environments within Fraunhofer AISEC:

- A deployment to a Kubernetes-based test platform, which also runs the Simulator and Evaluator components to provoke violations of metrics and requirements, to validate whether they are correctly represented in the Engine and Dashboard component
- A dedicated Docker-based deployment, which serves as a demo platform and continuously checks security metrics of internal services at Fraunhofer AISEC used in the development process of the Clouditor itself, such as the Jenkins CI server, SonarQube, Docker Registry and OpenStack.

Viability:

While the Clouditor development process already has a good set of unit and integration tests of individual modules, only rudimentary tests exist to automatically test the interaction between different modules. However, this is currently achieved manually by interacting with the deployments in the two test environments mentioned above.

The Clouditor Explorer, which is currently in development, will also allow a strong interoperability with existing cloud service APIs (such as OpenStack) through the automated discovery of certain parameters of cloud services (such as IPs, URLs), in contrast to a static configuration. Thus, Fraunhofer AISEC is currently assessing third-party libraries to access APIs of cloud services, such as the OpenStack, AWS or IBM Watson as well as multi-cloud libraries such as jcloud. After a successful integration of said libraries, the focus will be on the automated retrieval of a cloud services' components and the creation of appropriate Clouditor configurations.

MRL:

The prototype originated from a funded research project, which also included industry partners. This allowed for an initial input of metric and test cases that were developed in the prototype. Fraunhofer AISEC also started to validate these test cases outside of the initial research project by establishing contact to several cloud service providers as well as service customers and is currently in the process of feeding this input back into the development process. Additionally, first steps have begun to create a financial and business plan.

Conclusion:

We regard the Clouditor as TRL 4 with a strong indication that the prototype is moving towards TRL 5, especially once the already initiated steps such as the validation of test cases and financial plans have been completed.

3 ACTION PLAN - FURTHER DEVELOPMENT OF EXISTING TOOLS

In the following specific activities for each of the tools described above will be outlined in order to reach a higher TRL. According to the TRA Methodology (D1.1) this will be done in a structured manner covering the aspects

- description of the technology and the developmental efforts,
- the requirements derived from testing the technology,
- the environment in which the verification has taken place,

- the technology's viability and
- activities concerning the MRL of the technology.

As mentioned earlier the aim of this is to assure that the individual tools involved in the EU-SEC project reach a TRL of 7+ during the venture.

3.1 CLOUD TRUST PROTOCOL (CTP) SERVER

When it comes to the **description** of the technology, the interaction of the CTP with its environment, the description of the technology as a closed system, the differences of the functionality of the prototype and the laboratory scale tests as well as the implemented improvements derived from validating the prototypical system needs to be improved. Furthermore, the reactions of single components or subsystems to overload scenarios should be analysed and described and possible major bug eliminations need to be explained thoroughly.

Concerning the **requirements** of the technology, first an effort should be made, to take care of the missing or incomplete functionalities (e.g. notifications of cloud customers through XMPP messaging and the ability to represent relationship between several cloud services) Furthermore, the documented requirements of the functionalities need to be matched to different operating scenarios. According to different operating scenarios, specific parameters influencing the functionality of the technology should be named and outlined. In order to reach a TRL of 7 these operating scenarios should include real scenarios and if possible should contain the documentation of pilot tests in various realistic operating scenarios. Additionally, the requirements of the functionality of both external and internal interfaces need to be explained in detail.

The **verification** environment of the technology should move from the laboratory scales, to more realistic simulations and finally the real operating environment. The functionality in the real operation environment should be tested in at least one small scale (but real-life) case study with a pilot customer. Additionally the learnings drawn from these case studies need to be outlined concerning parameters of the operation environment.

Regarding the **viability** of the CTP potential deviations from the laboratory scale tests and the pilot tests concerning the functionality of the technology need to be analysed. In addition, the comparison of theoretical forecasts of the functionality and the actual functionality during the pilot test should be outlined. Furthermore, the effort of eliminating potential bugs compared to the added value for the technology's functionality should be explored and described.

In order to reach a higher **MRL** the feedback of potential customers of CTP should be taken into account in the further development of the technology. Specific suggestions made by potential customers should be implemented and tested. Furthermore, a market entrance strategy should be conceived covering the partnership with potential multipliers or major players, the most promising distribution channels, estimated revenue streams and brand / trademark registration.

3.2 CLOUDITOR

The **description** of the technology should be expanded and provide information of the validation of the prototype as well as potential learnings drawn from that. Implemented improvements need to be documented showing the further development of the technology and its single subparts in detail. Additionally, overload situations that occurred during the validation experiments have to be laid out and analysed for each subcomponent (e.g. the Clouditor Engine, the Clouditor Simulator and Evaluator, the Clouditor Explorer and the Clouditor Dashboard). The focus here should lay on metrics and conditions causing an overload on one side and learnings drawn from these overload situations for single subparts as well as the system as a whole on the other side.

In terms of the **requirements** concerning the functionality of the Clouditor the interfaces as well as the architecture surrounding the different subcomponents have to be analyzed and described more thoroughly. It would also be beneficial to lay out which adaptions of the system as a whole have taken place whilst the development of the prototype. Furthermore, according to the performance of the prototype, relevant parameters that are influential to the functionality of the prototype have to be identified. These could also be compared to parameters that seemed to be affecting the functionality of the system in previous laboratory scale experiments as this comparison provides information about unexpected factors. As also suggested for the CTP, a detailed description of the requirements needs to be given concerning multiple, diverse and realistic operational scenarios.

The most important progress in terms of the **verification** environment is the execution and documentation of one or more pilot studies with initial customers. These should be additional to the Kubernetes-based test platform and the Docker-based demo-platform. The operation scenarios, which are being used to test the performance of the Clouditor should be as realistic as possible. Any deviations between the tested operation scenarios and planned real-life operating scenarios must at least be named, should ideally be minimized however.

Concerning the **viability** of the Clouditor, the effort needed to advance from the actual method of testing the interaction between different modules (manually by interacting with the deployments in the two test environments) to the intended automatic evaluation has to be assessed. Furthermore, the expenditure of the integration of third-party libraries to access APIs of cloud services (e.g. OpenStack, AWS or IBM Watson as well as multi-cloud libraries) should be documented and evaluated in terms of its benefit for the system. According to the performance of the technology during the pilot(s), the effort needed to adapt the system to different operation scenarios and influencing parameters should be estimated. Also, the scope of potential bug elimination or error detection needs to be outlined.

Clouditor could reach a higher **MRL** by involving the mentioned industry partners even more in the development of the technology. Using structured and qualitative methods of gaining feedback in order to maximize the usability of the tool for potential customers might be considered. The activities concerning a financial and business plan could be extended to cover even more aspects of a potential business model such as a trademark registration, the identification of attractive sale channels and target markets.

4 RESULTING INNOVATIONS

Within the EU SEC Project the combination of different tools and schemes results in two highly promising and disruptive innovations. Each of them were generated as a result of the cooperation of the project partners representing potential customers, clients and providers of cloud service applications with very specific (security) requirements. In the following, these two innovations are described more thoroughly.

4.1 CONTINUOUS AUDITING BASED CERTIFICATION

Industry gap analysis has identified a lack of cloud services continuously providing up to date information on their compliance status to regulatory requirements and security standards. Financial institutions, like EU-SEC partner CaixaBank, are required to share sensitive information with regulatory authorities and other financial institutions. However, they are currently reluctant to use cloud services for these purposes, concerned about data management good practices by cloud providers. For this reason, the Continuous Auditing Based Certification aims at the continuous auditing of security requirements of cloud services with extraordinarily high safety standards such as in the financial and banking sector whilst reducing manual activities to a minimum.

The Continuous Auditing Based Certification relies on tools, methods and processes that allow for security properties of cloud services being checked with a frequency that can individually be defined and that only depends on the service level and qualitative objectives agreed upon between the parties, being involved in the certification process. Compared to a point-in-time certification, a continuous certification guarantees up-to-date results and a higher level of assurance to users and regulators. A continuous certification is achieved through a combination of automated and human lead auditing capabilities. Those are supported by the architecture for continuous auditing developed in the EU-SEC project, which facilitates the evidence collection, its evaluation as well as the publishing of the certification relevant information. Clouditor as well as CTP are covering significant aspects of this architecture, like evaluating evidence or handling the communication of assessment results.

In order to validate the functionality, as well as to assess the technology-readiness level of the Continuous Auditing Based Certification, two large-scale service implantations are being piloted. These pilots are being carried out with EU-SEC Partners such as CaixaBank, Fraunhofer AISEC and CSA. The pilot performs continuous auditing of a Financial Information Sharing application in the Cloud, which offers a service for the exchange of information between financial institutions and regulators with continuous control of the service requirements via an independent and autonomous audit system.

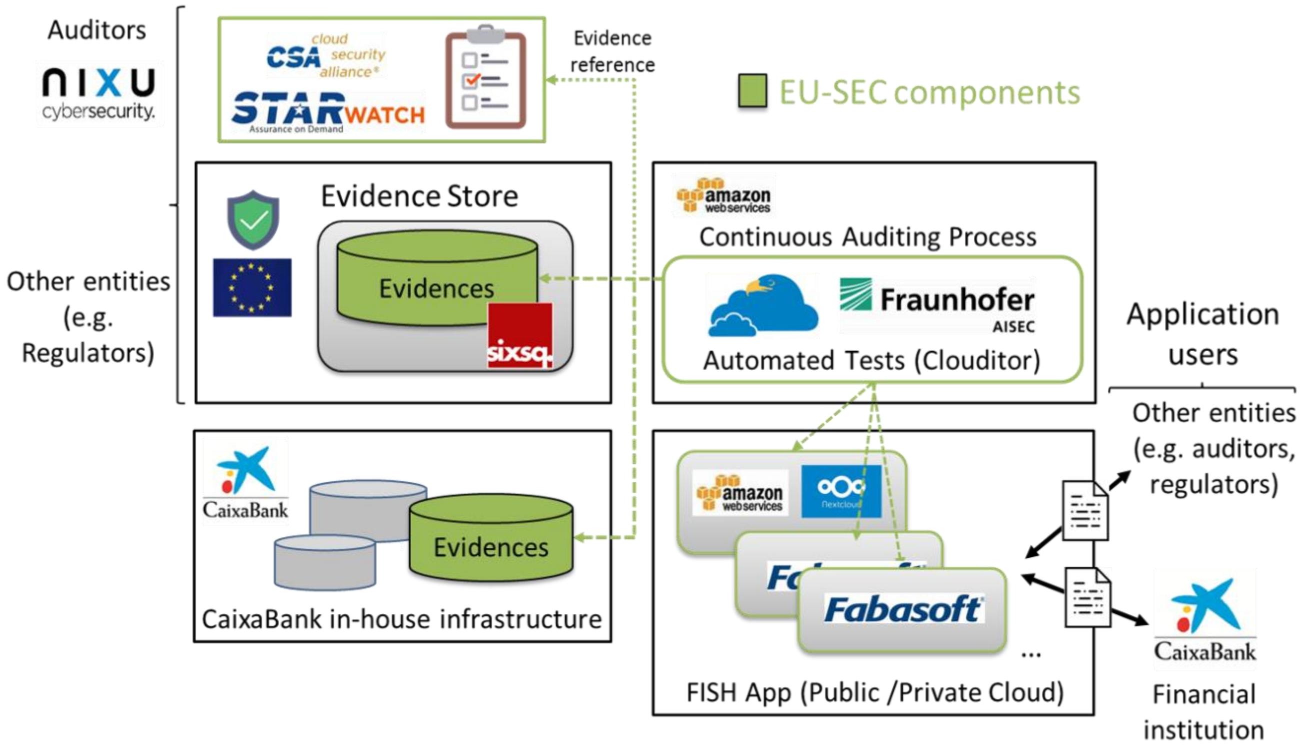

Auditors
nixu cybersecurity.
CSA cloud security alliance
STARWATCH Assurance on Demand
Evidence reference
🟩 EU-SEC components
Other entities (e.g. Regulators)
Evidence Store
Evidences
sixsq
amazon webservices
Continuous Auditing Process
Fraunhofer AISEC
Automated Tests (Clouditor)
Application users
Other entities (e.g. auditors, regulators)
CaixaBank
Evidences
CaixaBank in-house infrastructure
amazon webservices
Nextcloud
Fabasoft
...
FISH App (Public /Private Cloud)
CaixaBank
Financial institution

Figure 5: Technical architecture of Continuous Auditing Based Certification Pilots

4.2 MULTI PARTY RECOGNITION FRAMEWORK

Compliance with security standards is a must, but the confusing abundance of certification schemes in the cloud domain results in lack of transparency for cloud service providers, cloud users and regulators. In addition, the costs of compliance are huge. EU-SEC proposes a framework, approved by regulators, which will map and validate existing schemes.

The Multi Party Recognition Framework aims at streamlining a trustworthy recognition between different and partly overlapping cloud service security certifications. In this regard, the framework defines the principles, criteria, processes and technical capabilities for the mutual recognition between various national, international and sector specific cloud security certifications and attestations. The purpose of the framework is to address the problems of excessive proliferation of certification and attestation schemes, cloud providers' compliance fatigue and customers' confusion. Essentially, it makes the compliance and assurance market more effective and efficient. Synergies with continuous auditing are huge, even partly automation with tools like clouditor and CTP results in major efficiency improvements.

In order to validate the functionality, as well as to assess the technology-readiness level of the solution, four separate audit simulations are being conducted with EU-SEC partners. These involve a cloud service provider (Fabasoft), a cloud broker (SixSq), two public bodies (the Slovenian and Slovak Ministries), an ISAE auditing firm (PwC) and an ISO27001 Certification Body (NIXU). In this currently conducted pilot phase of the project, the mutual recognition embraces the requirements from BSI C5, CSA CCM, ISO27001, ISO27017, ISO27018, and SOC2 to enable the reusability of requirements between different certifications.

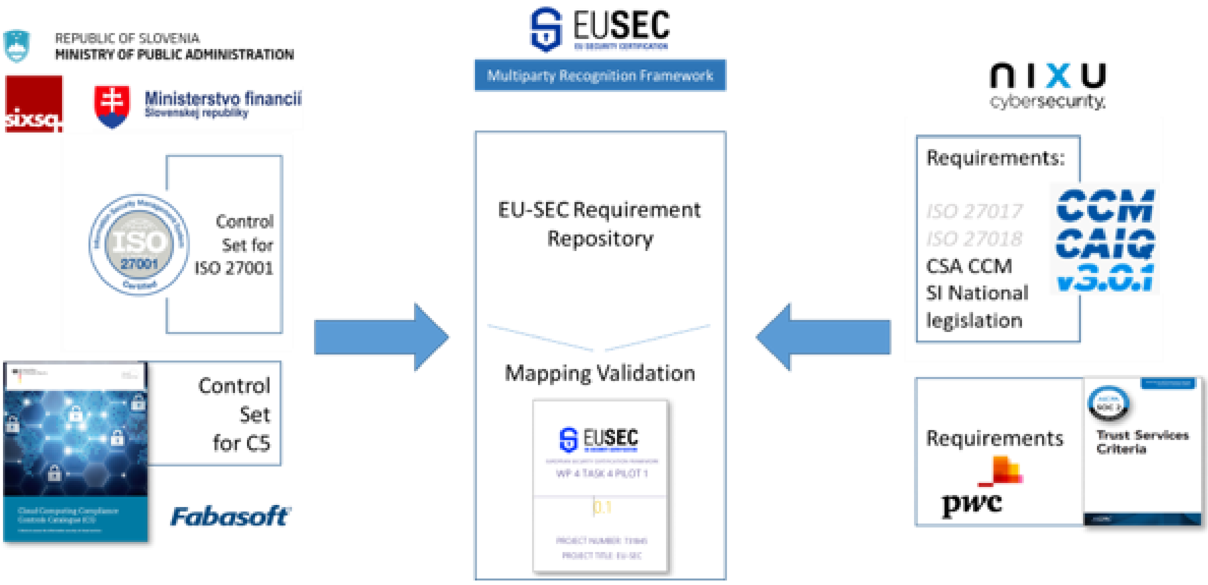


Figure 6: Pilot of Multi Party Recognition Framework

5 INNOVATION ACTIVITIES CONCERNING EXPLOITATION

In order to explore the exploitation potential of the two innovations described above, individual workshops will be conducted for the Continuous Auditing Based Certification as well as the Multi Party Recognition Framework. During this workshops both developers and potential customers or end users of each of the innovations - as represented by the different project partners - will work together to identify the most important aspects concerning the exploitation of the solutions. These aspects focus on the two main factors: First, the two products or innovations will be explored in terms of their core features and essential functionalities. Second, the building blocks of potential business models of the two innovations will be examined. To warrantee a comprehensive and structured way of gathering this information from the participating parties, the methods Value Proposition Canvas and Business Model Canvas will be implemented during the workshops. The following gives a detailed description of the applied methods.

5.1 APPLIED METHODS

5.1.1 VALUE PROPOSITION CANVAS

According to Alexander Osterwalder [1], the first step in the process of defining a product’s or service’s business model, is the identification of its value proposition. The value proposition aims at clarifying how a product or service meets the needs of a specific customer segment and therefore creates a value for the target group. Specifically, the core features and most important functionalities of a product are being identified and matched to the respective customer needs. In order to gather the information concerning the value proposition of a product systematically, the canvas showed in Figure 4 is used.

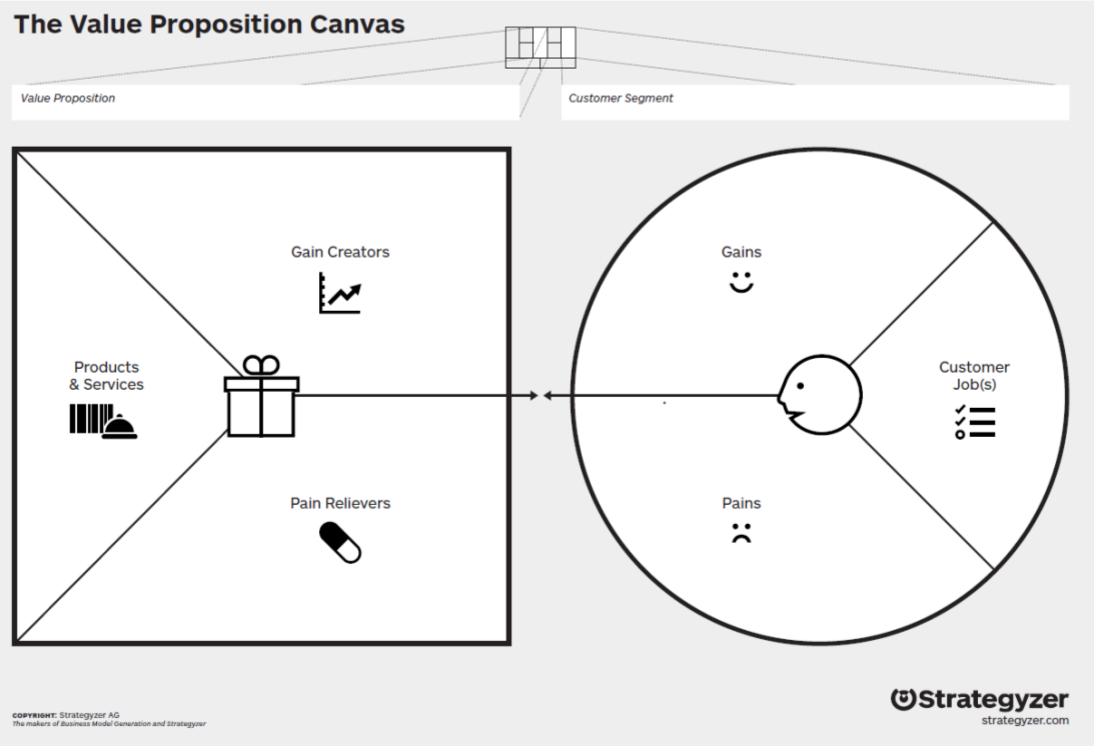


Figure 7: The Value Proposition Canvas by Alexander Osterwalder [8]

The Value Proposition Canvas, as shown in figure 4, is divided into two sides (the product / services side and the customer side), each of which is further subdivided into three fields or building blocks. The right side of the canvas deals with the targeted customer segment. The focus on this side lays on

1) the customers' job which they are trying to accomplish by using the product
2) the pains of the customers trying to fulfill the job and
3) the potential gains of the customers while fulfilling their jobs.

The customer job relates to the idea, that a product is never just used for the sake of using it, but for getting a specific task done. So here the purpose of the product from a users realm needs to be explored and explained. The customers' pains include all negative aspects that arise along the process of trying to get the specific task done. This negative aspects should ideally cover emotional, social and functional aspects and represent a negative way of expressing the customers' needs. The customers' gains, however, deal with all the potential positive aspects that could emerge while getting the specific job done. Just as for the customers' pains, the customers' gains should ideally cover all social, emotional and functional benefits that could come up along the process of trying to get the specific task done.

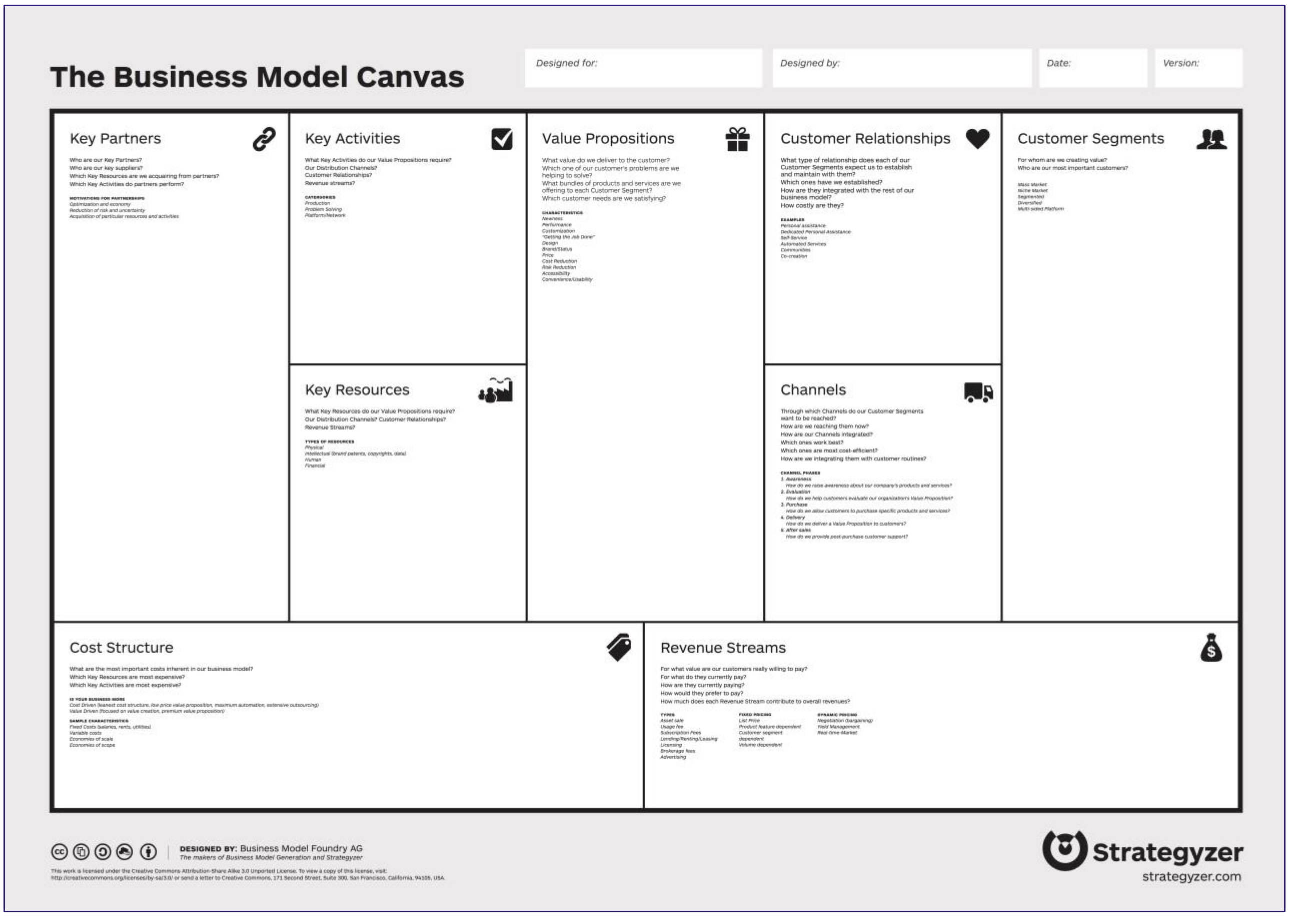
The left side of the canvas, however, deals with the product or service being developed. The three fields dividing this side are used to specify

4) The type of the product or service that will be offered to the customer in order to get their jobs done
5) The Pain Relievers, which are aspects or features of the product or service, which relieve the customers' pains and
6) The Gain Creators, which are aspects or features of the product or service, which create gains for the customers.

The type of product or service should provide information about the technical background or origin of the innovation. This should include an understandable and shortened description of the product, that makes clear, how the product can be used to get the defined customers' job done. The Pain Relievers give an insight into features or functionalities of the product, that cover the identified pains of the customer. Ideally, this results in a list of different aspects of the product that are necessary to solve the social, emotional and functional problems that arise for the customers whilst trying to get their jobs done by using the product. The Gain Creators, however, deal with all the positive aspects that the product could offer the customers whilst using it. Respectively this would ideally result in a list of features that makes it possible for the customers to fulfill their positive social, emotional and functional needs that emerge during the process of getting their jobs done by using the product. Here, however, the focus does not lie on core functionalities or features of the product but rather on nice-to-have aspects.

As the different fields and the content of the canvas indicates already, the aim of this method is to map the product and its features to existing customers' needs and desires. According to this method, however, the most important features of a product could vary from customer group to customer group. For this reason it is important to use the method rather as a guideline to collect customers' feedback during the development of a product and to be able to adapt the product and its features according to the feedback of each individual customer group if necessary. Furthermore, the definition of the value proposition represents the first step in the creation of a potential business model, as different aspects emerging during the definition of the value proposition might have an important impact on one or more building blocks of the business model [1].

5.1.2 BUSINESS MODEL CANVAS



The Business Model Canvas

Designed for:

Designed by:

Date:

Version:

Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquiring from partners?
Which Key Activities do partners perform?

MOTIVATIONS FOR PARTNERSHIPS
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities

Key Activities

What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?

CATEGORIES
Production
Problem Solving
Platform/Network

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

TYPES OF RESOURCES
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

CHARACTERISTICS
Newness
Performance
Customization
"Getting the Job Done"
Design
Brand/Status
Price
Cost Reduction
Risk Reduction
Accessibility
Convenience/Usability

Customer Relationships

What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?

EXAMPLES
Personal assistance
Dedicated Personal Assistance
Self-Service
Automated Services
Communities
Co-creation

Channels

Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?

CHANNEL PHASES
1. *Awareness*
How do we raise awareness about our company's products and services?
2. *Evaluation*
How do we help customers evaluate our organization's Value Proposition?
3. *Purchase*
How do we allow customers to purchase specific products and services?
4. *Delivery*
How do we deliver a Value Proposition to customers?
5. *After sales*
How do we provide post-purchase customer support?

Customer Segments

For whom are we creating value?
Who are our most important customers?

Mass Market
Niche Market
Segmented
Diversified
Multi-sided Platform

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

IS YOUR BUSINESS MORE
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)

SAMPLE CHARACTERISTICS
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope

Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

TYPES	FIXED PRICING	DYNAMIC PRICING
Asset sale	*List Price*	*Negotiation (bargaining)*
Usage fee	*Product feature dependent*	*Yield Management*
Subscription Fees	*Customer segment dependent*	*Real-time-Market*
Lending/Renting/Leasing	*Volume dependent*	
Licensing		
Brokerage fees		
Advertising		

DESIGNED BY: Business Model Foundry AG
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

Figure 8: The Business Model Canvas by Alexander Osterwalder [9]

The Business Model Canvas is a straight forward method to develop a business models or to adapt it to changing market situations or customer groups. Figure 5 shows the Business Model Canvas, which is divided into nine fields.

Each of the nine fields or building blocks deals with specific questions and specifications concerning the business model. The content of the individual fields can be derived from Table 2.

Table 2 Building blocks of a potential business model [2]

Building block	Questions	Specifications
Customer Segments	- For whom are we creating value? - Who are our most important customers?	Different Types of Customer Segments: - Mass market - Niche market - Segmented - Diversified

		- Multi-sides platforms
Value Propositions	- What value do we deliver to customers? - Which of our customer's problems are we helping to solve? - Which customer demands are we satisfying? - What products and services are we offering to each Customer Segment?	Following Elements can contribute to customer value creation: - Novelty - Performance - Customization - Getting-the-job- done - Brand/Mark - Price - Cost reduction - Risk reduction - Convenience/Usability
Customer Relationships	- What type of relationship does each of our customer segments expect us to establish and maintain with them? - Which are already established? - How costly are they?	There are several categories of Customer Relationships, which may co-exist in a company's affiliation with a specific Customer Segment: - Personal assistance - Self-Service - Automated Services - Communities - Co-Creation
Revenue Streams	- For what value is each Customer Segment truly willing to pay	Pricing mechanisms: - Fixed list prices - Bargaining - Auctioning - Market dependent - Volume dependent - Yield management A business model can involve two different types of Revenue Streams: - Transaction revenues resulting from one-time customer payments - Recurring revenues resulting from ongoing payments to either deliver a Value Proposition to customers or provide post-purchase customer support

Key Resources	• What Key Resources do our Value Propositions require? • Our Distribution Channels? • Customer Relationships? • Revenue Streams?	Categories: • Physical • Financial • Intellectual • Human
Key Activities	• What Key Activities do our Value Propositions, Our Distribution Channels, Customer Relationships and Revenue streams require?	Categories: • Production: designing, making, and delivering a product • Problem solving: new solutions to individual customer problems. • Platform/network: Networks, matchmaking platforms, software, and even brands can function as a platform
Key Partnerships	• Who are our Key Partners? • Who are our key suppliers? • Which Key Resources are we acquiring from partners? • Which Key Activities do partners perform?	Types of partnerships: • Strategic alliances between non-competitors • Coopetition: strategic partnerships between competitors • Joint ventures to develop new businesses • Buyer-supplier relationships to assure reliable supplies
Cost Structure	• What are the most important costs inherent in our business model? • Which Key Resources are most expensive? • Which Key Activities are most expensive?	Characteristics: • Fixed costs • Variable cost • Economies of scale (larger companies, profit from lower bulk purchase tariffs) • Economies of scope (one marketing department can support numerous products)

The individual building blocks should ideally be edited and processed in a chronological order from the top to the bottom of the table presented above. As mentioned before, the first two building blocks represent the definition of the value proposition. The reason for this is, that the value proposition can have an important effect on the other aspects of the business model such as customer relationships, key activities and key resources for example. Depending on the degree of the planned diversification of a product for targeting different customer segments, there can several value propositions and potential business models emerge [2].

5.2 PROCEDURE

The two methods described above will be implemented for the two innovations Continuous Auditing Based Certification and Multi Party Recognition Framework. For each of the innovations one workshop will be held to define the value proposition and one to define a potential business model.

During the Value Proposition Canvas workshops both developers and customers as represented by the EU-SEC partners will work together to gather the necessary information. After the customer jobs, pains and gains of the potential customers are explored, the description - and possible adaptions - of the innovations will take place by mapping the product and its features to the customers' information with the help of the specific product developers. For the Continuous Auditing Based Certification CaixaBank serves as a potential customer during the workshop, whereas Fraunhofer AISEC and CSA represent the developers of the innovation. For the Multi Party Recognition Framework Nixu, PwC, Fabasoft, SixSq, Ministry of Finance of the Slovak Republic and Ministry of Public Administration of the Republic of Slovenia serve as potential customers during the workshop, whereas CSA and NIXU represents the developer of the innovation. After the different features of the two innovations are described and listed, a poll will be conducted in order to identify the most important features of the innovations in the eyes of the EU-SEC partners.

During the Business Model Canvas workshops for both innovations the developers and potential customers will work through the single building blocks of a potential business model in a stepwise manner. It is expected that the EU-SEC partners representing the developers of the innovations will provide most of the information needed to define a potential business model. The EU-SEC partners representing the potential customers of the innovations, however, play an important role in validating certain hypothesis of the business model right away, such as potential distribution channels or targeted customer relationships for example.

6 CONCLUSION

Within the Innovation Management Plan, it could be shown that most of the tools being implemented in the EU-SEC framework have reached a TRL of 7+ according to the TRA Methodology (D1.1) already. The tools, which are not meeting this requirement, are the Clouditor and the CTP, which are currently evaluated with a TRL of 4 to 5. It was shown, however, that these tools can reach the intended TRLs during the project by implementing certain advancements and adaptions concerning

- the description of the technologies and related developmental efforts,
- the requirements derived from the latest functionality tests,
- the environments in which testing takes places and
- the technologies' viability as well as
- the activities concerning the MRL of the technology.

Furthermore, it could be shown that two new innovations emerged within the EU-SEC framework, which seem very promising in terms of a potential exploitation: The Continuous Auditing Based Certification, which represents an innovative auditing procedure, and the Multi Party Recognition Framework, representing a process innovation, that aims at reducing the auditing effort by streamlining various auditing schemes.

For these two innovations, activities concerning the further exploitation of these products were outlined. Namely, the implementation of the Value Proposition Canvas [1] and the Business Model Canvas [2]. Both methods will be applied in settings involving both the developers and the potential customers of the innovations as represented by the EU-SEC project partners.

REFERENCES

[1] A. Osterwalder, "Value proposition design: How to create products and services customers want," 2014, John Wiley & Sons;

[2] A. Osterwalder & Y. Pigneur, "Business Model Generation," 2010, John Wiley & Sons;

[3] P. Granig & S. Persuch, "Grundlagen des Innovationsmanagements,", 2012. [Online]. Available at: file:///C:/Users/ama/Downloads/9783834929532-c1%20(1).pdf. [Accessed: 15-December-2018];

[4] C. S. Alliance, "A new way to streamline and simplify cloud security compliance with STARWatch," 2016. [Online]. Available at: https://star.watch/assets/White_Paper_Final-92109763d18ab1d34477ae944690ebb7549f51186123b7ac13beef30cc8bf8d7.pdf. [Accessed: 15-December-2018]

[5] C. S. Alliance, "CTP Data Model and API," 2015. [Online]. Available at: https://github.com/cloudsecurityalliance/ctpd/blob/master/client/CTP-Data-Model-And-API.pdf. [Accessed: 15-December-2018].

[6] C. S. Alliance, "The CTP Backoffice Prototype API," 2015. [Online]. Available at: http://htmlpreview.github.io/?https://github.com/cloudsecurityalliance/ctpd/blob/master/client/CTP-Admin-API.html. [Accessed: 15-December-2018].

[7] V. Driessen, "A Successful Git Branching Model," 2010. [Online]. Available at: http://nvie.com/posts/a-successful-git-branching-model/. [Accessed: 15-December-2018].

[8] Strategyzer AG, "The Value Proposition Canvas,". [Online]. Available at: https://strategyzer.com/canvas/value-proposition-canvas. [Accessed: 15-December-2018].

[9] Strategyzer AG, "The Business Model Canvas,". [Online]. Available at: https://strategyzer.com/canvas/business-model-canvas. [Accessed: 15-December-2018].

[10] EU-SEC Deliverable D1.1, "EU-SEC TRA-Methodology"