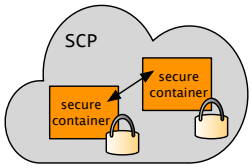
Information and Communication Technologies

H2020-ICT-2015



SECURE CONTAINER PILOT (SCP)

– ENSURING CONFIDENTIALITY, INTEGRITY, AND EASE OF USE OF CLOUD-BASED SERVICES –

Work program topics addressed: FTIPilot-01-2016
Type of action: Innovation Action
Coordinating person: Dr. Martin Süßkraut, SIL, Email: martin.suesskraut@silistra-systems.com
List of participants:

No.	Participant organization name	Short name	Coun-try	Type of organization
1 ***Coordinator***	SIListra Systems GmbH	SIL	DE	SME
2	SyncLab	SYNC	IT	SME
3	Exus	EXUS	UK	SME

Abstract:

Containers are becoming increasingly popular in private cloud environments. For example, Google alone starts every week more than two billion containers. Containers supports effective software packaging and effective utilization of computers. Modern container engines, like Docker, simplify the composition and management of applications. These features make containers ideally suited to build modern **cloud-native applications**.

The security of containers is, however, insufficient when containers from multiple cloud tenants must be protected when running in public or hybrid clouds and even in private clouds: for example, software vulnerabilities in the operating system can be exploited to access information in other containers. In addition, service developers must protect the confidentiality and integrity of data against accesses from all other parties, including the cloud provider itself.

The new Intel SGX CPU extension introduces the concept of a **secure enclave** which permits to protect code and data from accesses by other software, even when accessed by higher-privileged system software. We use SGX for a **secure container infrastructure** on top of Docker: all data at rest (e.g., on disk), in transmission (e.g., via Ethernet), and during processing (e.g., by a web services) is encrypted and protected from unauthorized accesses.

The SCP project will use this SGX-based secure container technology - which are currently at level TRL3 (experimental proof of concept) and extend this technology to TRL 7. The main objective is to evaluate the technology in an operational environment and ensure that the software satisfies all requirements needed in operational environments. We will evaluate this pilot in the following three contexts: 1) two flagship applications by partners SYNC and EXUS, 2) a trial of the SCP container platform with SMEs, and 3) adaptation of an external application to the SCP platform.

Table of Content

1. Excellence

SCP will increase the technical readiness level of a **unique secure container platform** to TRL7. This **SCP platform** is based on the popular **Docker platform**. Currently, more than 100,000 applications are running on top of Docker – despite being only a few years old. This steep uptake of Docker can be explained by the fact that Docker simplifies the **packaging** and the **deployment** of software. Containers are a virtualization mechanism implemented by the operating system. They are more light-weight than **virtual machines**. However, the security of Docker containers is lacking in comparison to virtual machines. The security of virtual machines is enforced with the help of hardware mechanisms like VT-x, APICv, VT-d and SR-IOV. So far, containers are only isolated by the operating system. SCP addresses this issue by executing containerized applications inside **trusted execution environment –** ensuring a **superior security isolation**. The SCP platform is based on Intel SGX, a novel CPU extension by Intel, that provides an application with a **secure enclave** which encrypts data and code and **preventing all accesses** except from the application itself.

The unique aspect of SCP platform is that it provides **application-oriented security**. Instead of focusing on the security of the hypervisor, the operating system, and the cloud, it ensures the security of an application such that one only needs to trust that the trusted execution environment of the CPU is correctly implemented. The research on which this work has been based was published in **the** premier systems conference[1].

With the arrival of novel **trusted computing hardware** on the mass market, in particular, Intel SGX, it is now possible to ensure secure computation at remote sites. This technological capability is a potential **game changer** considering that limited trust is one of the main inhibitors for outsourcing services to cloud environments. Intel SGX offers two essential technical contributions: (1) **remote attestation of the application code**, and (2) **confidentiality of data that is processed by the attested code**. SGX achieves data confidentiality by only decrypting data inside the CPU package. This approach protects it from unauthorized access by privileged users, such as system administrators, and is also resilient to common forms of physical attacks.

1.1. Objectives

1.1.1. Market Opportunity

According to Gartner, the market of IaaS has a size of US$22 billion in 2016[2] and will grow to US$59 billion by 2019. The market size of cloud application services (SaaS) is even bigger with US$37 billion in 2016 and is expected to grow rapidly. The cloud management and security services is smaller with about US$6 billion in 2016. The objective of the SCP platform is to address three markets: IaaS, SaaS as well as cloud management and security services – which has a total market size of more than US$65 billion in 2016 and all three segments are still growing quickly. We are in particular targeting the growth potentials in these markets which is predicted to have an **annual growth** between 14% and 17% percent.

1.1.2. Overall innovation project objectives

The SCP platform will be based on an existing secure container prototype (currently TRL3, i.e., experimental proof of concept) that has been developed within the H2020 projects SERECA and SecureCloud. The objective of SCP is to commercialize the platform within less than 3 years. We will

[1] S. Arnautov, et al, *SCONE: Secure Linux Containers with Intel SGX*, OSDI 16.
[2] http://www.gartner.com/newsroom/id/3188817

1) Increase the TRL of the **secure container platform to TRL7.** The platform is compatible with the Docker platform. Applications inside of a secure container are, however, executed inside of a trusted execution environment. All files and all communication are encrypted to protect the confidentiality and privacy of all application data and processing.

2) Ensure the security of applications inside of secure containers by **enforcing the memory safety of programs** with minimal overhead. Violations of memory safety are the main cause of intrusions like those based on infamous Heartbleed attack[3].

3) Provide **secure container images with guaranteed memory safety for popular applications**. Docker images of applications like **nginx**, **redis**, **postgres**, **mysql**, **mongo**, **gitlab**, **nginx-proxy**, **haproxy**, and **memcached** are very popular and have each been downloaded (i.e., "pulled") between 5 and more than 10 million times from *dockerhub*[4].

4) **Implement a business plan that is an extension of the business plan of Docker Inc**. Note that Docker Inc is currently valued at more than 1 billion US$ and its business model is based on service contracts for business customers. Our business model is three fold: a) maintenance contracts for secure container platform (similar to those offered by Docker Inc but for secure containers) and secure container images (see 3) (partner SIL), b) system integrators like SYNC will provide help to other companies to port their applications inside of secure containers, and c) application service providers like EXUS and SYNC will provide the software services inside of secure containers to be able to outsource these into the cloud to facilitate the scalability of their existing businesses without the risk of large hardware investments while protecting their IP and the application data.

1.1.3. Specific objectives

Secure containers are based on Intel SGX. This CPU extension permits to run applications such that all memory state is encrypted such that only the CPU knows the encryption key. Neither the operating nor the hypervisor can access the encryption key nor the state of an application protected with SGX.

Secure containers protect against attacks of an application via the operating system – even if the attacker has physical access to the computer. A hacker has, therefore, to attack applications directly. The attacker could, for example, exploit bugs within the application. To protect against such attacks, we need to ensure the memory safety of these applications. Protecting the memory safety is in general very expensive, in particular, even hardware extensions like Intel MPX have large slowdowns of up to x10 times. We have implemented a new approach with an average slowdown of only 20%. This mechanism needs to improved to TRL7.

Secure Container Image Service. Tuning applications with a competitive performance inside of secure containers is difficult – due to the limitations of the secure enclaves. This requires lots of knowledge and tuning skills. Hence, our objective is to commercialize this knowledge by providing secure container images of popular applications like **nginx**, **redis**, **apache** and **memcached** that are not only well tuned but also provide **memory safety** using a compiler extension protecting applications inside of enclaves. Access to these images are only granted to customers that pay a monthly service fee. In return, the client gets access to the newest versions of the service with the latest security patches.

Secure Container Platform. The SCP platform is based on the Docker platform. To be able to use the newest releases of Docker, we actually do not modify the Docker platform itself. To ensure that our secure containers are compatible with Docker, we

- compile the applications such that they can run inside of secure enclaves,

[3] https://en.wikipedia.org/wiki/Heartbleed
[4] see https://hub.docker.com/explore/?page=1

- encrypt and authenticate all application files that are part of a container image, only an application running inside a secure enclave has the access right (and key) to access these file, and
- all communication with the enclave is encrypted – not only all TCP connects but also *stdin*, *stdout* and *stderr* streams are encrypted.

Companies can sign service contracts to gain access to the newest version of the secure container platform. The support costs will be the same as those provided by Docker. For example, a **business day support** will cost $1000 yearly **per instance**, i.e., Docker engine running on a single physical or virtual computer. A **business critical support** will cost $2000 yearly per instance and will include 24/7/365 support.

Secure Container Cloud Services. To simplify the usage of secure containers, we will set up a cloud service for customers experiment and operate secure containers - to simplify the adoption of the SCP platform. We will charge for nodes running secure containers, initially, €150 monthly per node. This price will, however, need to be adjusted based on real costs and the availability of other clouds starting to offer SGX enabled machines.

Pilot flagship applications. Within the SCP project, our objective is to port the LivingMarket sub product of EXUS' flagship application **EFS**[5] of EXUS and the flagship application **StreamLog** of SYNC to secure containers. The reasons for moving these applications in secure containers are different. EFS was recently awarded as best-in-class globally and is a comprehensive suite of software applications that manages credit risk along the whole lifecycle of accounts, from the moment of disbursement until write-off or debt sale. EFS helps organizations/banks: (a) identify and treat credit risk early, (b) perform efficient collections, (c) manage legal proceedings and recoveries, and (d) gain detailed insight into portfolio evolution, collections strategies and resource efficiency.

Currently, the EFS roadmap plans the **migration of the software to the cloud** in order to facilitate a range of new features such as the ones of the LivingMarket product as well as a different business model. Clearly, the confidentiality as well as the integrity of the data processed by EFS must be protected. There are also the legal requirements that the data of EU banks must not leave Europe. In particular, this must be ensured even if a foreign government would get legal access to all user data hosted by a cloud provider[6]. Within SCP, we ensure that all data accessible by the cloud provider is encrypted. Within SCP, we will focus on porting on of the new security-relevant feature to secure container.

The flagship application of SYNC is StreamLog[7]. This application provides an effective approach for access control monitoring of system administrators. StreamLog audits the actions performed by system administrators to detect abuses. There is an increasing focus on this issue in Italy - as well as in Europe - in the last few years. Italian law mandates that abuses by system administrators be detected, the data owners are to be notified and these administrator be prosecuted in court.

There is a strong business case for porting the security critical parts of StreamLog to a secure container. The main motivation is to protect the **integrity of the collected and logged data**. A malicious system administrator would of course be highly motivated to tamper with the collected as well as with the recorded data. In its current implementation, StreamLog is - at least to some extent - vulnerable to such attacks by a smart system administrator. Hence, we need to protect the data collection and data storage features of the application from administrators with root access. We can do so by executing the collection and storage within secure containers. The presentation layer of the application has only read access to the data and can continue to run outside secure containers.

[5] http://www.exus.co.uk/en/products/debt-collection-software-suite
[6] http://www.zdnet.com/article/us-strikes-back-in-microsoft-email-warrant-case/
[7] http://www.synclab.it/prodotti/streamlog/

The parts of StreamLog that run in secure containers will be rewritten in C. StreamLog will be our pilot application to show the support for C-based applications as well as our compiler extension that ensures memory safety of applications running inside of secure containers. Both StreamLog as well as EFS will use the secure container images from SIL for a) a secure database backend, and b) for the secure web servers required to run inside of enclaves to protect the TLS certificates and to ensure the integrity and confidentiality of the communication.

1.2. Relation to the work program

Fast development, commercial take-up and/or wide deployment of sustainable innovative solutions in enabling and industrial technologies

SCP combines partners with complementary expertise and clearly identified contributions to create a unique and new value-chain: SIL provides secure container environment compatible with the fast growing Docker environment, SYNC and EXUS provides software as a service on top of secure container infrastructure complementing their applications with secure container images for web services as well as the data base. There is also large market for helping software companies to move their applications inside of secure containers by a) providing secure container images of standard applications (SIL), and b) providing services to help these companies to port the application for secure containers (SYNC).

...and/or for tackling societal challenges

SCP addresses the key societal challenge of increasing the level of protection of organizations against cyber-disruptions, data breaches and theft of critical information. This challenge has been recognized at world-wide level and while today senior executives consider cyber-security as a necessary cost 75%[8], surveys indicate a shift towards 59% considering cybersecurity as a competitive advantage within 3 years. This directly relates to the *Secure Society Challenge* and more specifically to the specific aim *Cyber Security for SMEs, local public administration and Individuals*

Time to initial market take-up no later than 3 years after the beginning of the FTI project.

SCP will develop an innovative secure container platform that will be demonstrated and evaluated in operative environments. This will become a market-ready platform by the end of the project. SCP implements a “go-to-market” scheme.

Enhanced competitiveness and growth of business partners in the consortium, measured in terms of turnover and job creation

We expect a substantial growth of all partners of SCP based on the exploitation of these results.

Increased industry participation, including SMEs, and more industry first-time applicants to Horizon 2020.

SIL is a first-time applicant.

1.3. Concept and approach

1.3.1. Overall Concept

Commercial approaches either cover only the secure storage of encrypted data within the cloud, and thus do not allow for any processing of that data within the cloud. Our approach utilizes novel CPU

[8] 2015- Global Megatrends in cyber security , Ponemon institute, published 02/2015

extension - Intel SGX.[9] This kind of hardware allows the execution of encrypted code on encrypted data where the corresponding plaintexts are only known inside the processor but will never leave it. The secure area in which the processing of the plaintext data happens is referred to as an "enclave".

Intel provides a SDK (software development kit) to build applications for secure enclaves. The idea of this SDK is that only parts of an application should be stored inside an enclave. Even for new applications this is an inconvenient approach. Splitting existing applications in two parts (data+code **inside the enclave** and data+code **outside of the enclave**) is a very difficult challenge: First, such a partitioning introduces performance overheads for entering and leaving the enclave. Second, one needs to define a new interface inside an existing application that provides access to the data and code kept inside of an enclave in a secure fashion. A reengineering of existing applications has proved to be extremely difficult. For example, many classes would need to be split in two – to keep the security relevant fields of an object inside an enclave and the remaining fields outside.

In contrast to the existing approaches, we support that a complete application will be executed inside an enclave. This eliminates the need to define a new interface of an application. In particular, we will support many popular applications can run inside of enclaves without reengineering. However, these applications need to be properly configured to ensure security and properly tuned to ensure sufficient performance. Often, both require intimate knowledge of these applications. To simplify to execution of such applications, we will provide a **container image service**. Popular service like **nginx**, **apache**, and **mysql** will be properly configured inside of a secure container such that all communication is encrypted (via TLS), all files are encrypted before leaving the enclave, and these applications are executed inside of an secure enclave.

Secure versions of popular applications will be provided in form of secure container images. Customers can configure and operate instances (i.e., containers) of these secure images only after signing up to a paid subscription services.

A secure container runs on top of an operating system. It is protected against attacks from/via the operating system call interface (so called **iago** attacks) by a) encrypting data to be stored on disk or transmitted via the network, b) performing all memory management of the application inside the enclave (required to protect against iago attacks), and c) performing a careful checking of all arguments of calls to the operating system.

Secure containers are also protected against attacks by hackers. Attacks on applications frequently use low level vulnerabilities like buffer overflows and return oriented computing. For example, the OpenSSL Heartbleed attack used such low level vulnerability of OpenSSL[10]. We have a compiler-based approach that protects applications inside of enclaves with minimal overhead (average is below 20%). This protection will only be available for **enterprise-level subscriptions**.

Secure containers are not only protected against accesses from system administrators, cloud providers and operating systems but also against low-level attacks by attackers with knowledge of application bugs that violate memory safety – which are the most common attacks. (This feature will require an enterprise-level subscription)

An application running inside a SGX secure enclave will suffer non-negligible performance overheads if its working set gets to large (currently, 90MB[11]). We will provide a software mechanism (with

[9] In the rest of this proposal we will use the acronym SGX (Software Guard Extensions) to refer to the needed security extensions of a given processor. Nevertheless, we will develop our solution to be as flexible as possible so that it can be adapted to any processor which offers the need security functionality—not just Intel processors.
[10] http://www.theregister.co.uk/2014/04/09/heartbleed_explained/
[11] this is the usable size of the EPC (extended page cache) of current generation SGX implementations – this will increase in the next generation of SGX.

enterprise-level subscription) that extends the supported working set size of applications by automatically keeping some state outside of the enclave.

Our compiler extension can transparently move application state of an application outside of a secure enclave. This mechanism is faster than the hardware mechanism because it use the actual object size instead of page size (which is 4KB). (This feature will require an enterprise-level subscription)

We will investigate the secure container approach in the context of two pilot applications. These pilot application will run as secure containers and will access standard secure container applications like **redis** and **mysql**, respectively.

1.3.2. Strategy and approach

Our strategy to ensure the success of SCP is that we focus on the following properties:

- **Ease of use**. The SCP platform is based on well-known Docker engine. The main complexity of the SCP approach is hidden in the generation of secure container images. Commonly used containers are made available via a **secure container subscription service**.
- **Security**. Applications will need to run in open systems like public clouds and might even stretch across multiple clouds for availability and scalability. SCP protects the confidentiality and integrity of applications using not only secure enclaves but also compiler extensions that protect applications against attacks. The compiler extensions are only available to **enterprise-level subscribers**.
- **Manageability**. Considering that applications will run across multiple clouds, one needs tools to simplify the management of these applications. Hence, SCP supports integration of secure containers within Docker Swarm to simplify the management of secure containers. Support of Docker swarm will require an **enterprise-level subscription.**
- **Transparency.** Enterprise-level subscribers can optionally get access to all source code that runs inside of enclaves via a **source-code subscription**. This subscription does not include the compiler that is used to protect and speed-up the execution of applications inside secure enclaves.
- **Ease of adoption.** To ensure to potential customers can simply try out secure containers, we will provide a cloud for experimenting and running secure containers.
- **Piloting sessions**. We implement an open call to SMEs interested in joining the piloting phase of SCP platform. This will include 20 piloting sessions in which the SME is expected to port one of their applications to secure containers. Resources to support these SMEs have been allocated to SIL, and direct financial support of 4.000 € / SME. In return, the SME is expected to create a secure container image of at least one application. The SME will, however, have to sign up for an enterprise-level subscription for the trial.

1.4. Ambition

Although cloud computing models offer several economic advantages compared to on-premise solutions, many enterprises are still reluctant to move their mission-critical applications and data to the cloud. One reason for this reluctance is the lack of trust in the security solutions offered by the cloud provider and the effort and skills needed to move applications to the cloud.

The SCP project provides a platform that simultaneously establishes trust and offers competitive performance through the use of secure containers. So far, no commercial offering is available that provides similar features as the SCP platform. SCP extends a modern container-based execution environment (Docker and Docker Swarm) and facilitates companies to move applications to the cloud not only by protecting the application but also by providing prepackaged secure container images for standard application components like the web service and the data base. We explain how the SCP project will advance the state-of-the-art in the following areas.

Challenge: Secure container-based application provisioning

The traditional model of running applications inside of virtual machines has several drawbacks: first, the acquisition of new resources through virtual machines introduces a non-negligible latency, making it impractical for applications that require low latency for the provisioning of new resources; second, running virtual machines including the full OS stack for potentially each micro-service introduces unnecessary complexity and runtime overhead. Other approaches to reduce the application's size, for example, library operating systems [20] or customized language/runtime systems[12] require the developer to adapt the application.

SCP adopts a container-based approach using the Docker framework. Docker-based application containers are typically an order of magnitude smaller and less complex than full virtual machines. A container-based approach provides greater flexibility to customers: application containers can be launched and restarted significantly faster than virtual machines. Containers are also a good match with modern cloud-native applications which need a lightweight mechanism to host the potentially large quantity of micro-services.

In SCP, we will improve the security of containers using novel CPU extension by Intel. There is no commercial nor academic approach yet that provides similar security guarantees. We combine the leanness, ease of use, and efficiency of containers with the security levels previously not even achieved by caged systems. A secure container includes a runtime environment which is encapsulated within an enclave to guarantee security. For the management of the containers we support Docker Swarm.

Challenge: Secure Standard Services

Very few applications are written completely from scratch. Instead, applications use standard services like a load balance (like **haproxy**), a web server (like **Apache** or **nginx**) and a storage service (like **MySQL** or **MongoDB**), and caching service (like **memcached**). We provide secure versions of common standard services running inside of secure containers.

SCP will reduce the effort of moving applications in secure containers by providing prepackaged container images of popular applications. These container images are tuned and configured such that these application protect all data that they transmit, process or store.

1.4.1. Relation to other European projects

Several European projects are linked to SCP. We focus on the two most closely linked EU projects:

Related EU project	How SCP extends beyond
The **SERECA**[13] **project focuses on secure reactive programming in public clouds with the help of SGX secure enclaves.**	The focus of SCP is on increasing the TRL of some artefacts created within. The focus of SCP is on exploitation of standard applications investigated by SERECA as well as the system support developed within SERECA.
SecureCloud[14] focusses on **secure container technology using SGX.**	SCP will use the secure container technology of SecureCloud and increase their TRL to ensure that they can be commercially exploited.

2. Impact

According to Cisco's Global Cloud Index Forecast, more than 30% of the cloud workloads will be in public cloud data centers by 2018. They expect the workflows in clouds to nearly triple between 2013

[12] http://zerovm.org/ and http://zerg.erlangonxen.org/
[13] http://www.serecaproject.eu
[14] https://www.securecloudproject.eu/

and 2018, while the workload of traditional data centers is expected to decline in the same period. If less than 40% of the Internet consumer population used cloud storage in 2013, by 2018, 53% of this population should be using it.[15] Goldman Sachs expected that spending on cloud computing infrastructure and platforms should grow at a 30% CAGR from 2013 through 2018, while overall enterprise IT should grow only 5%. They see spending in cloud infrastructure and platforms growing to $43 billion in 2018, in a global market for enterprise information technology that is larger than $300 billion.[16] According to Network World, security (36%), cloud computing (31%) and mobile devices (28%) are the top 3 initiatives IT executives are planning to have their organizations focus on.[17]

Europe is facing a crossroad regarding cloud adoption and security. SCP will provide a platform that addresses these cloud security challenges. The Forrester Forecast estimated that global SaaS revenues should reach $106 billions in 2016 (21% increase over projected 2015 levels). A report from security and governance firm Skyhigh Networks[18] provides evidence demonstrating that European enterprises use an average of 588 cloud services with just 9% providing enterprise-grade security capabilities and the remaining 91% posing a risk. Of the total 2,105 cloud services used by European enterprises, only 12% encrypt data at rest, 21% support multi-factor authentication, and 5% are ISO 27001 certified. The report also warns that shadow IT is "widespread and uncontrolled" and is 10 times more prevalent than companies assumed.

Confidentiality, integrity, availability and security of applications and their data are of immediate concern to almost all organizations which use cloud computing, and particularly to organizations that must comply with strict confidentiality, availability and integrity policies, including those supporting society's most critical infrastructures, such as smart grids and utilities in general, health care, and finance. Hence, there are a number of application domains that represent major business drivers for a massive take-up of security-enhanced cloud technology such as the one being developed by SCP.

2.1. Expected impacts

The outcomes of SCP project will produce breakthrough SCP platform for running service and applications inside clouds. The current situation is inappropriate for the applications currently deployed because it solely relies on the cloud provider's reputation concerning security. Therefore, the current service market in Europe is not able to sustain the evolution of a widespread ecosystem of cloud services because it lacks the security levels required to execute such services.

We foresee the SCP platform to be deployed within less than 2.5 years after project start. With the results of SCP, cloud-native applications running in secure containers will support current sensitive business and government applications such as healthcare, critical systems, banking, and voting. Considering its impacts on the European society and the rise of a corresponding service market, it is fundamental for European cloud infrastructure and service providers.

2.1.1. *Contributing to impacts from the work programme*

SCP is fully in line with the expected impacts set out in the work programme since:

- the novel SCP platform and SCP pilot applications will be quickly delivered. The first pilot sessions will start within at most 12 months and will reach the market through a wide deployment in less than 3 years

[15] Cisco Global Cloud Index: Forecast and Methodology, 2013–2018: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf
[16] http://news.investors.com/technology/011615-735080-amazon-aws-leads-in-cloud-msft-googl-crm-rising.htm
[17] Network World's "2015 State of the Network Study, Technology Adoption Trends & Their Impact on the Network": https://www.scribd.com/document_downloads/253406492?extension=pdf&from=embed&source=embed
[18] http://www.skyhighnetworks.com/cloud-report/

- it will strengthen the competitiveness and growth of the partners in the consortium and of providers and consultants external to the consortium, measured in terms of turnover and job creation
- it will directly support SMEs and large organisations to protect their IP and the confidentiality and integrity of their data and code.
- it will extend the market place for service providers to scale their businesses by using cloud services running inside of secure containers.

2.1.2. Users and Container Usage

Any potential user of containers and Docker is a potential user of the SCP platform since we provide compatibility with Docker while adding security by executing programs inside secure enclave and encrypting all files and all communication. To identify some potential customer, we can have a look at the customers of Docker. For example, ADP mentions the following challenges regarding their IT infrastructure[19]:

"*There are three key challenges that ADP faced. The first is security. Security is top of mind at ADP because they work with sensitive information. The US government considers ADP "critical infrastructure" because they hold data like over 55 million social security numbers and with all the payroll processing, in the last year they moved about 1.8 trillion dollars through the ADP systems. Roughly 10% of the GNP was moved four times through ADP systems and for the people reading this blog post right now, most of your social security numbers are sitting in an ADP datacenter*."

The approach to address this security challenge by Docker is based on signed images. The SCP platform supports signed images and **in addition** it a) attests all programs before they can start to ensure that only programs signed by the customer (in this case, this would be ADP) can run and can get access to credentials, b) it protects the programs against attacks, and c) ensures that all data is always encrypted. We therefore expect that in particular large companies like ADP will be interested in the SCP platform. Moreover, the SCP platform is compatible with Docker which simplifies the migration to the SCP platform substantially.

Docker is very popular and we expect that we can convince some of the Docker customers to use the SCP platform. As an indication of the popularity, the adoption of Docker (amongst Datalog customers) have grown during the last 12 months about 30%[20] and runs now on **about 10% of the hosts**. It is mostly run by companies with many hosts, i.e., the adaption rate is much higher for **companies that have 500+ hosts** than those that have only 100-500 hosts and even less for companies that have less than 100 hosts. There are multiple possible conclusion regarding this. One conclusion is *that Docker solves problems of companies operating a large number of hosts*. These companies, like ADP, have also the need to keep their data confidential. For such companies, we will provide an **enterprise subscription** for the SCP platform – for more details, see below.

Companies that adopt Docker, adopt it quite quickly. Some research shows that 2/3 that try Docker actually also adopt Docker for production. Most companies adoption within 30 days and almost all remaining companies within 60 days[20]. The lesson to be learned from this, is that companies are happy with the functionality that Docker provides. SCP must keep that ease of use – despite adding security features which in many cases can reduce the ease of use. We have to ensure that the SCP platform has from start the right feature set. Hence, we plan 20 pilot sessions to verify that SCP maintains the ease of use of Docker and the right set of security features.

Statistics from dockerhub[4] and datdog[20] show that several Docker images have a very high popularity amongst the Docker users. Many of these popular Docker container images need to preserve

[19] https://www.docker.com/customers/docker-datacenter-delivers-security-and-scale-adp
[20] https://www.datadoghq.com/docker-adoption/

confidentiality like databases like **mysql** and **postgres** or handle SSL certificates and user data like **nginx**. Hence, we address this popularity by offering secure versions of these container imagers as secure container images instead. Hence, we provide a **secure container image subscription** service for customers to be able to get access to well tuned versions running inside of secure containers.

As we have already mentioned, in particular, companies running a large number of hosts adopt Docker. Our focus for the pilot sessions and for the later market entrance is to provide an attractive option for SMEs with a large demand for computing resources. SMEs can reduce their capital investment in hardware by renting resources from cloud providers. So far, the limited security isolation of containers either forces these companies to run the containers inside of separate VMs or avoid to run containers. The SCP platform offers - in form of secure containers – a superior security isolation without the need for VMs or physical hosts.

2.1.3. *Economic Impact*

The business impact of cyber attacks alone in Europe is estimated at 61 B$ in 2015, with approximately 74% of EU small businesses experiencing some form of data breach each year. SME businesses especially are vulnerable to cyber threats as they typically lack the expertise and manpower to ensure cyber defences are current and relevant for their business needs. This situation is compounded by a lack of awareness of cyber threats by up to 1 in 3 SMEs surveyed, which is a key hurdle in adoption of cyber security strategies and tactics. Cyber insurance, a key tool to mitigate the impact of cyber threats, has a market penetration of approximately 35% amongst EU businesses, with only 19% of SMEs holding a cyber insurance policy. An UK government commissioned report by Price Waterhouse Cooper in 2015 estimates the average costs of a 'worst case' data breach for SMEs at 75,000 - 311,000 £.

With approximately 22 million SME businesses in the EU, most of whom have some digital footprint and therefore vulnerability to cyber threats, the potential market for SCP is large in volume, as is the impact of an effective and sustainably engaging SCP platform. European SMEs are responsible for creating 85% of all new EU jobs and provided two-thirds of the total private sector EU employment in 2015. The data breach costs estimated above are simply not sustainable for the majority of SMEs and negatively impact employment. The potential societal impact of SCP extends beyond helping safeguard jobs within SMEs to protecting personal identifying information (PII) of clients and business partners. CSP will be a vital tool in enabling these SMEs to safely maximise their use of digital economic channels, increase competitiveness and bring innovative new products and services to market.

A common theme amongst European SMEs aware of cyber threats is the perception of lost customer data as having the most impact on their business. This statistic reflects the needs revealed by SMEs:

- to access digital tools that enable growth of their business and enhanced competitive advantage
- to access expertise assisting them through the experience of adopting cyber security best practices
- to reduce the complexity of understanding cyber risk and cyber security landscapes

The SCP platform provides a new product that is compatible with the very popular Docker platform but provides superior security level.

2.1.4. Market analysis, assumptions and revenues

Our current business plan considers the following services for the SCP platform that are similar to that of Docker Inc:

- One **business day support** will cost €1000 **yearly per instance**, i.e., the SCP platform running on a single physical or virtual computer.
- A **business critical support** will cost €2000 **yearly per instance** and will include 24/7/365 support.

Note, however, that these service contracts focusing on the support of secure containers. The potential market for this is huge. According to one of the largest study regarding the usage of Docker[20], about 10% of the hosts run a Docker instance. This means there is extremely large potential market for the SCP technology.

As an extension of the Docker business model, we provide the following extensions.

- A **secure container image subscription** service. For each secure container image, one must sign up for a yearly contract. Combining this with a **business day support** this will cost €1000 **yearly per image.** Note that this comes on top of the support contracts.
- A **business critical support** for a **secure container image** costs €2000 **yearly per image.**

In particular, for companies running a large number of instances and images, we will provide an **enterprise-level subscription service**. This includes **business critical support** for images and instances. The price of this service will be negotiated. For enterprise-level subscriptions, we will have two further options:

- **Source code subscription**. Companies can get the complete source code – including the SGX runtime – to be able to analyse the code running inside secure containers. This will double the yearly price of each image.
- **Protected container image**. The memory safety of the secure container image is protected to protect against hacker attacks.

It is difficult to estimate the market size for secure containers. Given the current growth of the container market, we predict that secure containers could also become a billion € market within the next 5 years.

2.1.5. Alignment with EU strategies and policies

SCP is perfectly aligned with EU strategies and policies on cloud computing security, and in particular with the Digital Agenda for Europe (DAE), successor of the i2010 initiative, which is one of the main strategy pillars for building a thriving digital economy by 2020. Security is one of DAE main focuses, and it is tackled by several actions. Specifically, SCP will contribute to the following Digital Agenda actions:

- Action 28: Reinforced Network and Information Security Policy
- Action 29: Combat cyber-attacks against information systems
- Action 32: Strengthen the fight against cybercrime at international level
- Action 33: Support EU-wide cyber-security preparedness

2.2. Measures to maximize impact

SCP has identified a number of measures that will be taken to ensure that its results have the impacts described above. The reason why a multitude of diverse actions has been planned is the awareness that technical innovativeness is the foundation for impact, but it is not sufficient alone to guarantee that impact will actually be achieved. In this section, we first discuss the measures that project will take to achieve impacts.

2.2.1. Dissemination and exploitation of results

SCP will be ready for progressive commercialisation by the end of the project. To support this ambition, a full “go-to-market” strategy has been defined and will be refined and implemented within dedicated WP (WP5).

The draft plan builds on a number of activities, with defined actions, targets and associated KPIs. The plan will be refined at the start of the project through a dedicated task (T5.1) and revised twice during the lifetime of SCP. The final release of this plan will be taken up as one of the results of SCP to guide future exploitation strategy. The overall goal of the plan is to pave the way and support the market approach defined in Section 2.1.4.

A structured road-show is planed. The goal of the road-show is to present the SCP platform in short sessions. The road-show will be the preferred tool to address the multiplying channels identified through trade associations, clusters and sectoral groups. The road-show starts in month 12 and will continue until the end of the project. We plan a total of at least 20 roadshows during that perios.

2.2.2. Training and community building

To build a strong SCP community, we will organize in person training as well as online training for the SCP platform.

2.2.3. Initial dissemination plans

SIL, as the coordinator of SCP, will ensure all the activities aiming at maximizing projects impact to the research and industrial community. This will be accomplished by exploiting the existing communication channels in domains relevant to the scope of SCP. SIL will promote SCP's outcome in the following ways:

2.2.4. Expected exploitable results & Preliminary exploitation plans

2.2.4.1.SIListra Systems GmbH

SIListra Systems GmbH will offer several services and subscriptions with respect to the SCP platform: we have already described these in Section 2.1.4.

2.2.4.2.Sync Lab

Sync Lab will exploit the SCP technology in the StreamLog product.

Competitor analysis

Widely speaking, any product/service that is able to provide forensic evidence of the "Seven Ws" (Who did What, When, Where, Where from, Where to, and on What) can be – at least in theory – be configured to become a potential competitor of Streamlog. Currently, the main candidates include: 1) IBM Tivoli Compliance Insight Manager; 2) CA Enterprise Log Manager; 3) Net IQ Log Manager; and 4) Engineering Netx. All the aforementioned products have two main drawbacks: i) a high Total Cost of Ownership (TCO), and ii) vendor lock-in.

Streamlog market penetration will be implemented through a structured offer, focused on a progressive uptake strategy. The new secured version of Streamlog will be available in four formats:

1. StreamLog Freemium – register and take a free tour of the service, to get insights into the benefits that are brought about by the possibility of tailoring Streamlog to the business and industry segment specific needs. The collected data is not saved.
2. StreamLog Solution Lite – low cost (<100€ monthly fee) license for small businesses. The company profile is saved and dynamically updated based on a user friendly GUI. Targeted alert service features and educational content is also available.
3. StreamLog Solution+ - (500€ monthly fee) as above, but with full connectivity and SIEM and system level monitoring (including support for common COTS products), full access to educational content and addition of forensic capabilities for tracking and reporting of abuses. Available as a cloud solution (SaaS) or on-site installation.
4. StreamLog Premium – (5000€ for initial installation and configuration + 700€ monthly fee) as above, but with the addition of correlation capability with the physical domain (e.g. IP video surveillance), for a truly holistic approach to activity monitoring. Targeted at larger SMEs and large companies.

The revenue stream includes:

- Direct licensing revenues: from Solution Lite to Premium.
- Annual fee from external consultants: an annual fee of 150 € has been computed. This low fee ensures crowd-sourcing of expertise. StreamLog creates a real opportunity for outside consultants, assuming that 2% of users will require 1 day of consulting per year.
- Commission on deployed solutions: solutions deployed to support an organisation through StreamLog will pay a commission fee. Low estimates have been done, based on an assumption of 2% of licensed users (details on this computation are not included here for sake of space, and due to the fact that in the model above this revenue stream represents less than 10% of the revenue streams).

As to cost analysis, marketing costs have been computed based on an acquisition cost of 100€ per new user and 200€ per new provider/consultant joining the "StreamLog community". Other costs relate to the equipment and FTEs required for support and operation of the platform.
The employment growth includes:

- Direct opportunities in a product line dedicated to the new StreamLog: the "customer support" employment growth provides 5 new FTEs over 5 years (this figure is conservative with respect to Sync Lab's growth in the last 5 years).
- Opportunities spread across the external consultants, with 6.120 days creating the equivalent of more than 40 FTEs, using a conversion ratio of 150 consulting days per consultant (each consultant has to retain days for training, information and preparation work).

StreamLog will mainly be offered to the Italian market, where the recent regulations (specifically: the November 2008 and the December 2008 (G.U. n. 300) mandating compliance to D. Lgs. 196/2003 represents a major market booster. We explicitly emphasize that the obligation to comply to the aforementioned directive applies to virtually all IT companies, as well as to the PA. According to our initial and conservative market penetration and growth estimations we anticipate an 80+% ROI after 4 years in the domestic market. As of the second year of commercialization, 20% of the revenues will be invested in Sync Lab development department for developing customization of the new Streamlog for the EU market.

2.2.4.3.EXUS

EXUS will exploit the SCP technology in the LivingMarket product which addresses SME retailers. The rationale behind their selection is the large number of SME retail businesses (520,000 in the UK) and the high completion they experience, which urges for accurate market and customer insights in order to improve their decision making processes. The feedback we had from discussions with several UK SME retailers, indicates their willingness to pay ~£1000 per year for a market & customer insights service, which draws upon actual financial data. This price is very competitive considering the alternatives and is in line with the £24,000 average annual marketing costs paid by SMEs, according to the Centre for Economics and Business Research. Thus, LivingMarket's annual Total Addressable Market is approximately £0.5bn for the UK.

Against competitors, LivingMarket has strong potential for adoption and market penetration. In a summary, existing solutions for market insights do not support features such as multi-dimensional analysis capabilities, near real-time analyses based on actual transactional data, merchant-level granularity; and importantly, an anonymization framework that safeguards the privacy of the data. Thus, existing offerings are incomplete and practically unusable beyond being able to provide to SMEs with a generic market overview. On the other hand, these and more features are supported by LivingMarket, providing a competitive advantage for market success.

According to our initial and conservative market penetration and growth estimations we anticipate a 97% ROI after 5 years in the market with ~4909 domestic SME retailer customers, which amounts to the conservative 0.9% market share in the UK.

Apart from the UK, we also plan to market our service in other European markets and also in Gulf Countries (GCC) and SE Asia (ASEAN) markets.

The strategy to develop our market share entails financial organizations as a reliable channel to market and offer our service to SMEs. Undeniably, banks, card processors and acquirers are seeking new digital services to complement their offerings not only for extra revenue, but also to address the threats imposed by fintechs' (see McKinsey's article 'Strategic choices for banks in the digital age'). Thus, we will exploit with financial organizations the distribution and joint promotion of the LivingMarket service, since no equivalent service is offered: only 2 out of the 10 biggest acquirers (including banks) in Europe offer rudimentary market reporting. Out of the 2nd-tier acquirers, only one is offering an ad-hoc reporting service based on a filled-out form. Moreover, banks will benefit from deeper insights into their SME clients, in order to improve their credit risk assessment.

2.2.5. Research data management plan

2.2.5.1.Policy for Data Management

SCP plans to participate in the Open Research Data Pilot. To cover that aspect a Data Management Plan (DMP) is periodically issued, to detail what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. A first version of the DMP will be provided at the sixth month of the project, and two updates are planned at month 20 and 30. Furthermore, if necessary, additional releases of this deliverable will be provided. The consortium plans to deposit data in a research data repository, and will take measures to enable third parties to access, mine, exploit, reproduce, and disseminate the data free of charge.

2.2.5.2.How data will be exploited and/or shared/made accessible for verification and re-use

The data will be shared after proper processing, aiming at removing any information that could be mapped to the identity of real people, via accurate (pseudo-) anonymization techniques. Anonymized data will be made available via multiple channels, and in particular: 1) it will be posted on the project Web site, in an area that will be accessible to the followers of the SCP project; 2) it will be shipped on digital support upon request (and compilation of a form); 3) it will be deposited in a research data repository, from which external users will be given the possibility to access, mine, exploit, reproduce and disseminate it free of charge; 4) it will be shared within the context of possible future initiatives promoted by the EC. Some of the data is governed by a very stringent and cumbersome set of legal requirements that restricts its use for research. However, anonymized data that demonstrate the use of the system can be made available given that all legal requirements are fulfilled.

2.2.5.3.How will data be curated and preserved

The data will be curated with respect to the relevant legislation, securing sensitive information and preventing private's data eavesdropping. For each use case the corresponding provider will store the original data locally at their respective premises. Data curation will include augmenting the data with associated metadata, for specifying the semantics. Data preservation will be ensured by having the Coordinator and the Technical Coordinator each store a copy of the original data at their respective premises. The data will be stored, archived, and preserved for the duration set by the legal framework.

2.2.6. Communication activities

The consortium has great confidence in its ability to produce high quality deliverables and disseminate the project findings based on their considerable past experiences, as shown by the

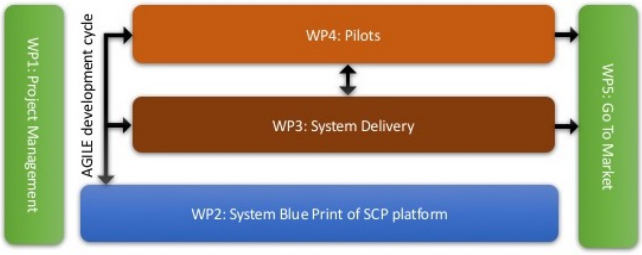
further information listed in partner profiles enclosed in the proposal. More complete lists of the consortium's related experiences and publications can be found on the websites of the individual partners. Furthermore, two of the three partners have participated in previous EU funded projects, exhibiting high involvement in communication initiatives.

3. Implementation

3.1. Work plan — Work packages, deliverables and milestones

3.1.1. Overall strategy of the work plan

The project has been structured around 5 work packages to deliver a market-ready integrated environment within 30 months, supported by a road show to reinforce the exploitation activities through pre-existing market channels as well as the innovative business models created by the solution space.



WP1 - project management - combines classical management with an agile technological management using SCRUM *methodology* and 2 weeks-long sprint runs. It also finalizes IPR and licensing aspects of the SCP platform, and manages the ethical issues.

WP2 – system blue-print – defines all details of the unified environment to deliver a market-ready solution, open interfaces, as well as the piloting approach in terms of scenarios and corresponding KPIs. It is a short duration work package, whose output feeds to WP1, 3, 4 and 5.

WP3 – *system delivery* – implements the overall environment, both at the level of each individual element and at the level of the overall integration. It delivers the platform and final version and the APIs.

WP4 – piloting – validates SCP platform through trials, by users / customers and by providers. For the user pilots, we will involve SMEs as users selected through an open call. Financial (4.000 € distributed to each SME) and human support is foreseen for up to 20 SMEs. The open call and the selection are managed by WP5. Therefore, a total of 20 testing sessions focused on users of the SCP platform. In addition to these 20 sessions, a continuous trial channel will be opened. This continuous trial channel will be linked in with our development sprints. We will identify at least one beta-tester for each of our pilot applications in the "go-to-market" section. The evaluation phase uses the requirements defined in WP2. The different pilots will focus on different angles:

- the 20 SMEs sessions will focus on ease of use at all levels (deployment, configuration, adaptability, information presentation) of deploying applications using secure container platform.
- the continuous trial channel will focus on the two flagship pilot applications being evaluated in the context of large organizations.

Piloting will also evaluate the usability of SCP for moving existing applications into secure containers.

WP5 – go-to-market – focuses on all activities to create visibility, enlist users (including beta-testers), generate interest and concrete uptake of software houses and service providers and creates the full online support resources for users. In addition, a road-show is organized by the project.

3.1.2. Timing of the different WPs and their components (GANTT Chart)

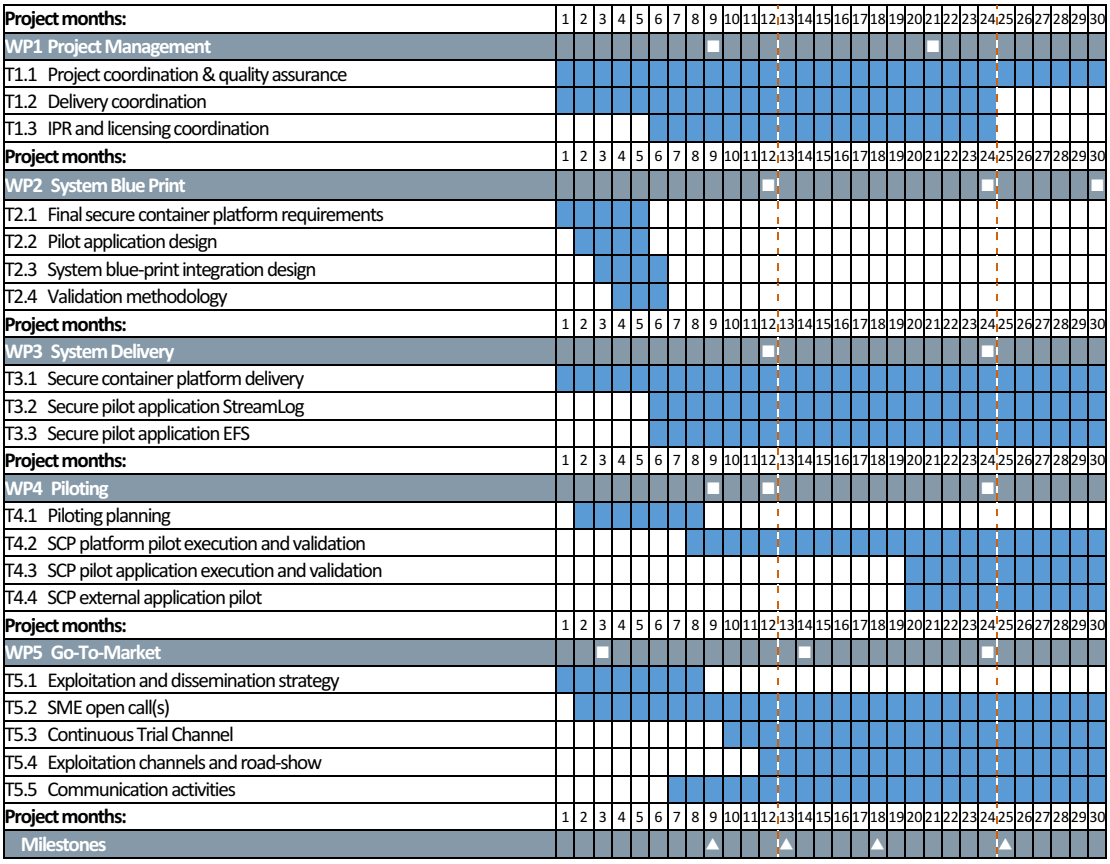


Table 3.1-1: Gantt Chart

3.1.3. Detailed description of work packages

	1	**Start Date or Starting Event**		M1
WP title	***Project management***			
Participant number	**1**	2	3	**Total**
Name of participant	**SIL**	SYNC	EXUS	
PMs	**20**	5	5	**30**

Objectives

- coordinate the project, support the implementation to ensure a market ready solution and manage the ethical issues. In addition to the administrative and overall coordination activity in task T1.1, two tasks are also included: the delivery management (T1.2) as well as the IPR management task 1.3. The full management structure is detailed in Section 3.2.

Description of work

T 1.1: Project coordination & quality assurance *(Months:**M1-M30,** Partners: **SIL (task leader), all)***

This task focuses on the project coordination in terms of processes, reporting, risk management and

quality assurance. It also includes the provision of an online collaboration tool to the consortium partners, provided by partner SIL. It integrates the management of the work related to ethics.

T 1.2: *Delivery* coordination (Months: **M1-M24** / *Partners*: **SIL (task leader), all)**

This task focuses on coordinating the complete delivery of the project, using the SCRUM based agile methodology covering 2 weeks sprints. This is the central coordination task from the "solution to market" point of view, it operates as the focal point between all activities and is referred to in several tasks in the detailed description of the work packages.

T 1.3: IPR and licensing coordination (Months: **M6-M24** / Partners: **SIL (task leader), all)**

The IPR approach requires a technology transfer from TU Dresden to SIL for the current prototype and a licensing approach between the partners. This task will focus on refining the details of the licensing between partners, and prepare the terms of use of SIL. Another key contribution of this task is to refine the business models based on the lessons learned during the project.

Deliverables

D1.1 (Report, Other): Processes, reporting guidelines and online tool (Editor: SIL, Delivered: M1, Related task: T1.1 and T1.2)

This deliverable contains the complete management information to consortium partners, including deliverable templates, organization of online tool, risk management, SCRUM methodology and quality assurance mechanisms.

D1.2, D1.3 (Report): Annual management reports (Editor: SIL, Delivered: M12, M24)

These are periodic complete project management reports, including the overall coordination information from task 1.1, the delivery coordination information from task 1.2. D1.2. will also include ethical information.

D1.4 (Report): IPR and licensing report (Editor: SIL, Delivered: M12, Related task: T1.3)

This deliverable defines the complete IPR and licensing schemes. It also defines the legal terms of the use of the secure container environment by partners and defines the allocation of revenues to partners for the use and reselling of the secure container environment.

D1.5 (Report): Updated IPR and licensing scheme (Editor: SIL, Delivered: M30, Related task: T1.3)

This deliverable is the final report for IPR and licensing, distributed as an online content in the "legal and licensing terms of use" of the SCP platform.

WP no.	2	**Start Date or Starting Event**		M1
WP title	***System blue-print***			
Participant number	**1**	2	3	**Total**
Name of participant	**SIL**	SYNC	EXUS	
PMs	**18**	10	10	**38**

Objectives

Defines the directions of the SCP platform and the SCP pilot applications. As a result, this WP will define the entries of the product backlogs for the SCP platform as well as of the pilot applications. To come up with the three backlogs, we first define all details of the SCP platform as well as how the two pilot applications will be build using the platform. This definition ranges from how to build a

secure container image, to configuration of secure container image, to description of APIs that permit to automate the creation, shipment and deployment of secure container images. This work package creates an output (in particular, the product backlog) that feeds back into the WP1 coordination activity to support the full development life-cycle of the SCP platform and the pilot applications through an agile development methodology (SCRUM).

Description of work

T 2.1: Final secure container platform requirements *(Months:* ***M1-M5*** */ Partners:* ***SIL (task leader), all)***

This task focuses on finalizing all the requirements, including detailed definition of the interfaces, comprehensive workflow definition and APIs (in particular, extensions of the Docker APIs) for the secure container platform. This will also come up with a list of standard containers that we will support and this defines the configuration of these standard containers.

T 2.2: Pilot application design *(Months:* ***M2-M5*** */ Partners:* ***EXUS (task leader), all)***

This task focuses on defining how to move the pilot applications to the secure container platform. This requires a careful analysis that determines which application components need to run in secure containers, which of these components need to be adjusted to be able to run inside of secure container, which need to be rewritten and which could be replaced by standard secure containers.

T 2.3: System blue-print integration design *(Months:* ***M3-M6*** */ Partners:* ***SIL (task leader), all)***

This task focuses on the integrated architecture, and delivers the complete blue-print of the SCP secure container platform and the application pilots. It will in particular include documentation of the workflows to integrate applications with the SCP secure container platform. The objective is that this can be used as a template for the integration of other applications.

T 2.4: Validation methodology *(Months:* ***M4-M6*** */ Partners:* ***SYNC (task leader), all)***

This task focuses on defining the validation, including scenarios for the pilots, the definition of a continuous trial channel, and KPIs used at each step to quantify the validation.

Deliverables

D2.1 (Report): Final SCP Requirements (Editor: SIL, Delivered: M6, Related task: T2.1)

This deliverable contains the set of final SCP requirements and details the interaction among the SCP elements, as well as the APIs for interoperability with clients of the secure container platform. This deliverable will contain the product backlog of the platform.

D2.2 (Report): SCP application designs (Editor: EXUS, Delivered: M6, Related task: T2.2)

This deliverable includes the definition of SCP pilot designs. This encompasses, in particular, the description of the secure components, their secure configuration and their secure interaction with other components and the integration with the SCP coordination services and a product backlog for each of the two pilot applications.

D2.3 (Report): SCP Blue-print (Editor: SIL, Delivered: M6, Related task: T2.3)

This blue-print contains the SCP platform architecture that is used as main input for the validation methodology in task 2.4 and for the System delivery WP. It provides an initial documentation of the workflow documentation.

D2.4 (Report): Validation approach and KPIs (Editor: SYNC, Delivered: M6, Related task: T2.4)

This deliverable defines the SCP validation methodology; it also refines the final set of KPIs based on the ones introduced in section 1.1.

WP no.	3	**Start Date or Starting Event**		M1
WP title	***System delivery***			
Participant number	**1**	2	3	
Name of participant	**SIL**	SYNC	EXUS	**Total**
PMs	**60**	30	30	**120**

Objectives

Deliver the SCP platform and SCP pilot applications. The delivery phase is managed through task 1.2, both for *the* successive releases and the updates linked to the results of the validation results coming out of WP4. It is important that task 1.2 will also manage the changes that could be brought to the system blue-print. This means that WP2 provides the initial blue-print, while task 1.2 will manage the product backlog and full development life-cycle done within WP3. The task includes both the secure container platform (driven by SIL) and the pilot applications running on top of the platform (driven by SYNC and EXUS).

Description of work

Task 3.1: Secure container platform delivery *(Months: **M1-M30** / Partners: **SIL (task leader), all)***

The objective of this task is to improve the TRL of the existing container platform TRL3 to at least TRL7. This task will be driven by SIL and will increase the TRL with the help of SYNC and EXUS. In particular, SYNC and EXUS will in particular provide instant feedback on any development decisions and providing input regarding the priorities of the product and sprint backlogs used in delivering the platform. This task will start already in M1 to increase the stability of the existing platform – which is needed for starting the delivery of the pilot applications. As soon as the product backlog is defined (in WP2), this task will also start develop or modify features based on the decisions made in WP2.

Task 3.2: Secure pilot application StreamLog *(Months: **M6-M30** / Partners: **SYNC (task leader), all)***

The objective of this task is to adapt and extend the StreamLog flagship application of SYNC to run this on top of the SCP platform. The product backlog of the adapation of StreamLogis defined in WP2. The selection of the sprint backlog and the update of the product backlog is driven by Task T1.2. This task is driven by SYNC. Partners SIL and EXUS provide instant feedback regarding any development decisions. SIL will help, in particular, with decisions influenced by the platform and EXUS regarding the application. The close interaction of the partners to ensure that the partner learn from each other to more effectively drive the platform and pilot application delivery.

Task 3.3: Secure pilot application EFS *(Months: **M6-M30** / Partners: **EXUS (task leader), all)***

The objective of this task is to adapt and extend the EFS flagship application of EXUS to run this on top of the SCP platform. The product backlog of the adaptation of EFS is defined in WP2. The selection of the sprint backlog and the update of the product backlog is driven by Task T1.2. This task is driven by EXUS. Partners SIL and SYNC provide instant feedback regarding any development decisions. SIL will help, in particular, with decisions influenced by the platform and SYNC regarding the application. The close interaction of the partners to ensure that the partner learn from each other to more effectively drive the platform and pilot application delivery.

Deliverables

D3.1: Platform Implementation Report *(Editor: SIL, Delivered: M7, Related task: T3.1)*

This deliverable summarizes the changes of the SCP platform and describes the state of the implementation of the SCP platform after the first 6 months.

D3.2: Platform and Application Implementation Report *(Editor: SYNC, Delivered: M16, Related tasks: T3.1, T3.2, T3.3)*

This deliverable summarizes the changes of the SCP platform and the pilot applications during the first 15 months. It focuses on the changes of the three product logs since the definition of the initial product backlog.

D3.3: Final Platform and Application Implementation Report *(Editor: EXUS, Delivered: M30, Related tasks: T3.1, T3.2, T3.3)*

This final deliverable of WP3 summarizes the changes of the SCP platform and the pilot applications during the first 20 months. It describes the final feature set of the SCP platform and the pilot applications.

WP no.	4	**Start Date or Starting Event**		M2
WP title	Piloting			
Participant number	**1**	2	3	**Total**
Name of participant	**SIL**	SYNC	EXUS	
PMs	**40**	20	20	**80**

Objectives

Test the resulting platform and pilot applications of three customer domains: 1) potential users of standard secure images like mysql or nginx (task 4.2), 2) towards new or existing customers of the two pilot applications (task 4.3), and 3) towards application developers that want to adapt their applications to run inside of secure containers (task 4.4).

Description of work

T 4.1: Piloting planning (Months: M2-M8 / Partners: SYNC (task leader), all)

This task has two parts. During the first month, an initial planning will be defined to be provided to task 5.1. Starting at month 6, a fully detailed planning will be worked out, based on the output of task 2.4. The planning focuses on the 2 iterations of the piloting activities (tasks 4.2 - 4.4). The planning includes: format of each piloting session, KPI measurement process, structure feedback to be taken account by task 1.2.

T 4.2: SCP platform pilot execution and validation (Months: M8-M30 / Partners: SIL (task leader), SYNC)

This task implements 20 sessions of piloting of the SCP platform and the standard secure container images. The early start of this task allows the preparation of the trial environments based on the

work carried out in the context of WP2.

T 4.3: SCP pilot application execution and validation (Months: M20-M30 / Partners: EXUS (task leader), SYNC)

This task tests the two SCP pilot applications with selected customers to evaluate how the new security features of the applications can benefit customers. In the context of the EFS application, to what extend customers are now willing to run EFS application in the cloud and more importantly, to accept a hosted version of EFS – despite contains very sensitive data. In the context of StreamLog, the piloting focuses on the added protection against potential attacks by malicious system administrators.

T 4.4: SCP external application pilot (Months: M20-M30 / Partners: SYNC (task leader), SIL)

This task focuses on how to help external companies to move their applications to the SCP platform. The focus of this task is to find a customer and to help this customer to move their application to the SCP platform. SYNC will focus on learning how to provide support for the adaptation of applications and SIL will focus on providing better platform support for this adaptation.

Deliverables

D4.1, D4.2 (Report): Pilot Plan (Editor: SYNC, Delivered: M1, M8, Related task: T4.1)

This deliverable has two versions. The first version (D4.1, M1) contains an initial planning useful to kick-off the work of task 5.1, while the second one (D4.1, M8) will contains the full pilot plan to coordinate tasks 4.3 and 4.4.

D4.3, D4.4 (Report): Pilots Execution Report (Editor: SYNC, Delivered: M15, M30, Related task: T4.2, T4.3, T4.4)

This deliverable reports about the execution and validation of the platform, application and external application pilots. The deliverable is issued in two versions, the first providing an initial report and the 2nd is the final pilots execution report.

WP no.	5	**Start Date or Starting Event**		M1
WP title	***Go-to-market***			
Participant number	**1**	2	3	
Name of participant	**SIL**	SYNC	EXUS	**Total**
PMs	**30**	20	20	**70**

Objectives

Define and create all the activities to reach-out to users and providers and pave the way to go-to-market with the complete environment. All activities that involved external organizations are created and managed through this work package. The approach to go-to-market has been defined at proposal time, and will be refined in task 5.1. The coordination of the activities are done by task 1.2.

Description of work

T 5.1: Exploitation and dissemination strategy *(Months:* ***M1-M8*** */ Partners:* ***SYNC (task leader), all)***

This task focuses on detailing the go-to-market approach in terms of approach and planning. It covers the refinement of the business pricing strategy (section 2.1.4), the steps to involve users during the project, the identification of all the exploitation channels and the supporting communication activities. The methodology will build on T1.3 (specifically D1.4 issued at M6) to ensure that the licensing and IPR solutions are aligned to exploitation. The approach impacts the definition of the the exploitation and dissemination strategy; this strategy is implemented by tasks 5.2 to 5.7.

T5.2: SMEs open call(s) (**Months*****: M2-M30 /*** *Partners****: SIL (task leader), all)***

This task defines and organizes two open calls to identify SMEs who will participate in the two piloting iterations. The approach is to select 5 to 10 SMEs in the first call. The selection criteria include profile of SME in terms of level of expertise in IT, security relevance and fitting application willing to migrate to a secure container or combine their application with one of the standard secure container. The task foresees a first call such the first piloting sessions start no later than M12; a second call will be organized not later than 12 months after the first call. The 2nd call will select more SMEs for a total of 20 SMEs. The decision when to organize a second call will be taken within task 1.2 following the finalization of the first set of piloting sessions. The decision will be based on the time when the changes of the SCP platform from the first pilot session will become available. This tasks includes the effort to handle the piloting sessions.

T5.3 Continuous Trial Channel (Months: M10-M30, Partners: SYNC (task leader), EXUS)

We will identify at least two large organizations that are willing to participate in an application pilot session. At least one application pilot session will be started for each of the two flagship applications.

T5.4: Exploitation channels and road-show *(Months:* ***M12-M30*** */ Partners:* ***EXUS (task leader), all)***

This task implements the communication activities to present, promote and foster market uptake through the exploitation channels identified in T5.1. A dedicated road-show will also be implemented jointly by the partners, under the coordination of a dedicated road-show manager.

T5.5: Communication activities *(Months:* ***M7-M30*** */ Partners:* ***EXUS (task leader), all)***

This task implements the communication activities to present, promote and foster market uptake through the exploitation channels identified in T5.1., using the exploitation and dissemination plan defined in T5.1.

Deliverables

D5.1 (Report): Exploitation and dissemination strategy (Editor: SYNC, Delivered: M8, Related task: T5.1)

This deliverable describes the methodology used by the project to ensure a coordinated approach to the market.

D5.2, D5.3 (Other): SME Call (Editor: SIL, Delivered: M12, M24, Related task: T5.2)

This deliverable is the open call to identify the SMEs who participate in the piloting activities. The deliverable may take different forms, depending on the channels used to announce the open call. A second version of the deliverable (D5.3) will be issued no later than M24, as detailed in task 5.2 above.

D5.4, D5.5 (Report): Communication activities (Editor: EXUS, Delivered: M12, M30 Related tasks: T5.3, T5.4 and T5.5)

This deliverable reports all the communication activities carried out, including the exploitation channels, continuous trial channel, and the road-show. It also analyses the KPIs linked to the go-to-market strategy and updates the strategy elaborated in T5.1 as necessary.

3.1.4. List of Work Packages

WP	WP title	Lead no.	Lead participant	Person months	Start month	End month
WP1	Project management	1	SIL	30	1	30
WP2	System blue-print	1	SIL	38	1	6
WP3	System delivery	1	SIL	120	1	30
WP4	Piloting	2	SYNC	80	2	30
WP5	Go-to-market	3	EXUS	52	1	30
				320		

Table 3.1-2: List of Work Packages

3.1.5. List of Deliverables

Del. no.	Deliverable name	WP no.	Lead part.	Type	Dissem. level	Delivery month
D1.1	Processes, reporting guidelines and online tool	1	SIL	R,OTHER	CO	1
D1.2	Annual management reports	1	SIL	R	CO	12, 24
D1.3	Annual management reports	1	SIL	R	CO	12, 24
D1.4	IPR and licensing report	1	SIL	R	CO	12
D1.5	Updated IPR and licensing scheme	1	SIL	R	CO	30
D2.1	Final SCP Requirements	2	SIL	R	CO	6
D2.2	SCP application designs	2	EXUS	R	CO	6
D2.3	SCP Blue-print	2	SIL	R	CO	6
D2.4	Validation approach and KPIs	2	SYNC	R	CO	6
D3.1	Platform Implementation Report	3	SIL	R	CO	7
D3.2	Platform and Application Implementation Report	3	SYNC	R	CO	16
D3.3	Final Platform and Application Implementation Report	3	EXUS	R	CO	30
D4.1	Pilot Plan	4	SYNC	R	CO	1,8
D4.2	Pilot Plan	4	SYNC	R	CO	1,8
D4.3	Pilots Execution Report	4	SYNC	R	CO	15,30
D4.4	Pilots Execution Report	4	SYNC	R	CO	15,30
D5.1	Exploitation and dissemination strategy	5	SYNC	R	CO	8
D5.2	SME Call	5	SIL	OTHER	CO	12,24
D5.3	SME Call	5	SIL	OTHER	CO	12,24
D5.4	Communication activities	5	EXUS	R	CO	12,30
D5.5	Communication activities	5	EXUS	R	CO	12,30

Table 3.1-3: List of Deliverables

3.2. Management structure and procedures

3.2.1. Organizational structure and Decision making procedures

The challenging objectives of the SCP project require a strong yet flexible management structure, supported by agile decision-making mechanisms, not only for the overall guidance of the project's activities, but also for interlinking all project components and optimizing liaison with the European Commission.

The project management structure has been designed to coordinate all components involved to ensure that SCP:

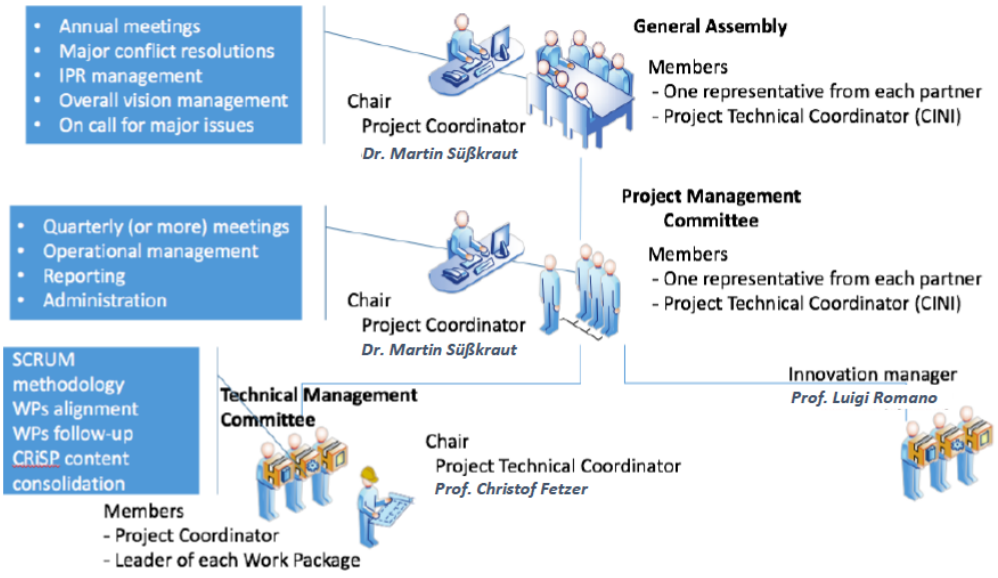
- attains the established project objectives according to the TRL 7 expectations
- maintains full process quality assurance
- takes advantage of using proper monitoring and self-assessment procedures
- aligns to legal, ethical, security, privacy and usability guidelines
- supports the implementation of the SCRUM methodology.

The SCP Project Management structure shown above has been agreed among the partners and is based on a similar model already implemented with success in past European projects.

- Strategic and vision management: **General Assembly.**
- Administrative, financial, overall coordination: **Project Management Committee**.
- Technical and content coordination, SCRUM product owner role: **Technical Management Committee**.

These committees have periodic face-to-face or virtual meetings (at least once a month). This organizational structure has been agreed to optimize planning, monitoring and coordination of SCP project activities, tasks performance, reporting and accountability.

3.2.1.1. Key Roles and Committees



The project will be implemented under the executive management of the **Project Coordinator (PC),** who will ensure the overall co-ordination and daily supervision and monitoring of operations and official communication with the European Commission (EC). He has the overall responsibility as well as for the financial and contractual obligations defined in the contract with the Commission. The PC is also responsible for making sure that IPR terms and conditions specified by the Consortium Agreement are properly interpreted. The Project Coordinator is **Dr. Martin Süßkraut** from SIL.

The Project coordinator will be supported by the **Technical Coordinator (TC)** and the **Innovation Manager (IM).** The **TC**, in the person of **Pr. Christof Fetzer** from SIL, will have the overall responsibility of ensuring

content synchronization between the different SCP outcomes in order to achieve the whole project goals; the TC will chair the **Technical Management Committee (TMC)**, responsible of ensuring the timely progress of the project and the high quality of the results. The **IM,** in the person of **Prof. Luigi Romano** from SYNC, will be responsible for the coordination of the SYNC exploitation and innovation process and management, coordinating the business exploitation of the outcomes of the technical activities and matching them to business opportunities.

The **Project Management Committee (PMC)**, led by the Project Coordinator, is the executive body of the project and it will have the responsibility of the management of the project, from the administrative, financial, technical and the user impact points of view. To this end, the Project Management Committee will comprise one representative from each partner, the PC and the TC. The PMC reports to the **General Assembly**, the highest decision-making body of the project, where each partner is represented, responsible for major administrative decisions, for solving potential disputes and for managing the IPR framework. Each work package will have a **work package leader (WPL)**, who will be responsible for organising and managing the work within the WP, including detailed planning of tasks and activities, the technical solution, the persons responsible for specific activities and the control of results including deliverables and milestones.

MS no.	Milestone name	Related WPs	Estimated date	Means of verification
MS 1	System blue-print complete	WP2	M6	D2.3 available
MS 2	SCP platform released for 1st pilots	WP3	M12	First platform prototype available
MS 3	SCP platform released for 2nd pilots	WP3	M16	Second platform prototype available First prototype of two pilot applications
MS 4	SCP platform and pilot final release	WP3	M30	Final version of SCP platform and pilot applications available

Table 3.2-1: Scheduling of milestones

3.2.1.2.Appropriateness of the Organizational Structure

SCP will deploy best practice innovation management methods to realize an extensible and flexible product closely oriented to market needs. The project will be closely connected with users throughout the value chain and with emerging technical developments in order to improve the different underlying components of SCP, but also to ensure that the modes of interaction of users with the platform take into consideration feedback coming from users through the extensive piloting phase. The innovation manager will ensure that the go-to-market strategy implemented through WP5 is aligned to the actual features delivered by WP2, WP3 and WP4. To ensure that relevant opportunities are identified and responded to, all consortium members will contribute to exploitation meetings (co-scheduled with ordinary TMC meetings).

3.2.2. Risk Management

The SCP project management team will perform a continuous risks evaluation throughout the project, in order to identify in time risks and contingency plans for mitigating their impact. A preliminary risk assessment has been carried out and reported in the following table in order to identify the most relevant risks and their contingency plans.

Description of risk	WP	Analysis of risk / Counter-measures
Partner withdraws or is unable to provide a foreseen contribution	All WPs	This risk has a very low probability of occurrence since SCP builds on a comprehensive strategy that is fully aligned to the business interests of all partners.

Lack of coherence in project development / lack of cooperation	All WPs	The platform details have already been worked out extensively and adherence to the plan will be monitored during the project. The use of the agile methodology directly supports early detection of any potential issue.
Project overspending	All WPs	SCRUM methodology to focus on the highest priorities features to ensure minimum impact on objectives despite limited budget.
Critical deliverables are delivered too late and milestones are missed.	All WPs	Management processes include specific roles for the monitoring and management of general, technical and human/legal/privacy/end-user issues and tasks, in order to timely detect potential problems and respond efficiently. Partners involved in tasks that might experience delay will allocate additional resources to meet the planned deadlines. The delivery schedule is very tight, which is why the SCRUM methodology was selected.
Problems related to IPR	All WPs	IPR and licensing issues have been addressed prior to SCP, and the driving principles agreed upon. The structure of SCP is such that the exploitation of the SCP platform is performed by SIL and the pilot applications by EXUS and SYNC, respectively. A license for the SCP platform to EXUS and SYNC will be granted.
Platform cannot be implemented within foreseen time and cost.	WP2, WP3, WP4	SCP will build on existing assets and solutions, which are an integral part of partners' core activity and thus of their priorities. The business interests of the partners are aligned to project objectives, and all partners will invest for the final delivery if needed.
Required components not available.	WP2, WP3, WP4	The components already exist – though at a lower TRL. Hence, this risk is very low.
Competition delivers a solution that makes SCP obsolete before reaching the market	WP5	SCP is positioned in a huge potential market – in which there is room for a number of players.

3.3. Consortium as a Whole

The SCP consortium builds on complementarity and full coverage, namely:

- the consortium provides the *full coverage of expertise and solutions to deliver the SCP platform and the pilot applications*
- each partner brings to the project its specialized and relevant *prior expertise* in order to improve the overall excellence of the consortium, to speed up the execution, and to increase the scope of SCP
- for the partners providing a prototype to SCP, *prototypes have been already evaluated at least at TRL-3*
- the European dimension is addressed both from the partners' geographical coverage and at the level of the target societal benefits of reducing the impact of cyber-disruptions, a major European challenge

3.4. Resources to be committed

Resources are well balanced, with 45% of the efforts dedicated to piloting and exploitation (WP4+WP5), and 47% to the delivery of the innovative solution (WP2+WP3).
Furthermore, task 1.3 in WP1 also contributes to the delivery with its contribution to IPR and licensing schemes:

Partner	WP1	WP2	WP3	WP4	WP5	total	%
SIL	20	18	60	40	30	168	50%
SYNC	5	10	30	20	20	85	25%
EXUS	5	10	30	20	20	85	25%
total (PM)	**30**	**38**	**120**	**80**	**70**	**338**	100%
%	9%	11%	36%	24%	21%	100%	

The total requested EC funding is **€ 2.359.875.** The distribution of costs and requested funding amongst the partners are as follows:

Partner	Financial Information			
	Cost	%	Funding	%
SIL	€ 1.678.750,00	50%	€ 1.175.125,00	50%
SYNC	€ 846.250,00	25%	€ 592.375,00	25%
EXUS	€ 846.250,00	25%	€ 592.375,00	25%
Total	**€ 3.371.250,00**		**€ 2.359.875,00**	

Three partners have "other costs" in total of €330.000 which is less than 10% of the total costs:

Total amount other costs	167000	82000	82000	
Description	SIL	SYNC	EXUS	Details in part B
Audit costs (€)	7000	7000	7000	EU requirements
Dissemination costs (exhibits)	35000	35000	35000	Section 2.1
SME pilot support	80000			20 SME piloting (€4000 each)
External cloud costs	10000	5000	5000	SGX-enabled hosts
Travel costs (see details below)	35000	35000	35000	
Conferences	4	4	4	
Project meetings	5	5	5	
Reviews	2	2	2	
Roadshow meetings	20	20	20	
Piloting sessions	20	20	20	