

*Information and Communication Technologies*

*H2020-ICT-2015*



Secure Container Pilot (SCP)

*– ensuring confidentiality and integrity and ease of use of cloud-based services –*

**Work programme 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 organisation name** | **Short name** | **Coun-try** | **Type of  organisation** |
| **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 microservice-based 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 private clouds: 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 public/hybrid/private 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 will use SGX to build 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 these SGX-based secure container technology - which are currently at level TRL3 (experimental proof of concept) and extend this technology to TRL 7 within the duration of SCP. 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 context of three domains: 1) in the context of a logistics domain, 2) in the context of access control system of system administrators, and 3) in the context of a backend banking service.

**Table of Content**

[1. Excellence 4](#_Toc464897095)

[1.1. Objectives 4](#_Toc464897096)

[1.1.1. Market opportunity 5](#_Toc464897097)

[1.1.2. Overall innovation project objectives 5](#_Toc464897098)

[1.1.3. Specific objectives 5](#_Toc464897099)

[1.2. Relation to the work programme 8](#_Toc464897100)

[1.3. Concept and approach 9](#_Toc464897101)

[1.3.1. Overall Concept 9](#_Toc464897102)

[1.3.2. Strategy and approach 10](#_Toc464897103)

[1.4. Ambition 11](#_Toc464897104)

[1.4.1. Relation to other European projects 12](#_Toc464897105)

[2. Impact 12](#_Toc464897106)

[2.1. Expected impacts 15](#_Toc464897107)

[2.1.1. Alignment with EU strategies and policies 18](#_Toc464897108)

[2.2. Measures to maximise impact 18](#_Toc464897109)

[2.2.1. Dissemination and exploitation of results 19](#_Toc464897110)

[2.2.2. Training 19](#_Toc464897111)

[2.2.3. Initial dissemination plans 19](#_Toc464897112)

[2.2.4. Expected exploitable results 19](#_Toc464897113)

[2.2.5. Preliminary exploitation plans 20](#_Toc464897114)

[2.2.6. Research data management plan 20](#_Toc464897115)

[2.2.7. Communication activities 21](#_Toc464897116)

[3. Implementation 21](#_Toc464897117)

[3.1. Work plan — Work packages, deliverables and milestones 21](#_Toc464897118)

[3.1.1. Overall strategy of the work plan 21](#_Toc464897119)

[3.1.2. Timing of the different WPs and their components (GANTT Chart) 22](#_Toc464897120)

[3.1.3. Detailed description of work packages 23](#_Toc464897121)

[3.1.4. List of Work Packages 29](#_Toc464897122)

[3.1.5. List of Deliverables 29](#_Toc464897123)

[3.2. Management structure and procedures 30](#_Toc464897124)

[3.2.1. Organisational structure and Decision making procedures 30](#_Toc464897125)

[3.2.2. Risk Management 33](#_Toc464897126)

[3.3. Consortium as a Whole 34](#_Toc464897127)

[3.4. Resources to be committed 34](#_Toc464897128)

# Excellence

SCP will increase the technical readiness level of a **unique secure container platform** to TRL7. This container platform is an extension of the popular **Docker platform**: more than 100,000 applications are running on top of Docker[[1]](#footnote-2). 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. The 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 are enforced with the help of hardware mechanisms like VT-x, APICv, VT-d and SR-IOV. Contain not only to justify its use in public and hybrid clouds but also in private clouds. SCP addresses this issue by executing containerized applications inside **trusted execution environment**. We use Intel SGX, a novel CPU extension by Intel, that can provide an application with a trusted execution environment which is called a **secure enclave**.

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 independent such that it only needs to trust the CPU, i.e., that the trusted execution environment is properly implemented[[2]](#footnote-3). The research on which this work has been based was published in **the** premier systems conference[[3]](#footnote-4).

## Objectives

**Confidentiality, integrity, and availability** of applications and their data are of immediate concern to almost all organizations that use cloud computing. This is particularly true for organizations that must comply with strict confidentiality, availability and integrity policies, including those which process **personal data** and those supporting society’s most **critical infrastructures** such as **finance** and **logistics**.

Until recently, the technological means to protect data while also allowing efficient computation have been limited. A common approach to mitigate the risk of data misuse is to contractually force the service provider to adhere to secrecy. Unfortunately, contractual agreements are ineffective in preventing determined attackers from stealing sensitive information. An example is a recent data breach at a subcontractor of T-Mobile that exposed millions of customers to potential identity theft[[4]](#footnote-5). T-Mobile, together with its subcontractor, is now the target of at least five class action suits related to the data breach. Even though legal delegation of responsibility has merit, it does not address the underlying technical causes of data breaches and identity theft.

With the arrival of novel **trusted computing hardware** on the mass market, in particular Intel SGX[[5]](#footnote-6), it is now possible to secure computation over sensitive data 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 as well as to client-owned devices. 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 onlydecrypting data inside the CPU package. This approach protects it fromunauthorized access by privileged users, such as system administrators, and isalso resilient to common forms of physical attacks.

### Market opportunity

According to Gartner, the market of IaaS has a size of US$22 billion in 2016[[6]](#footnote-7) 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 further. The cloud management and security services is with about US$6 billion in 2016 smaller. 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 already more than US$65 billion in 2016 and all three segments are 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.

### 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 SecureCloud H2020 project. The objective is to commercialize the platform within less than 3 years. To do so, we will

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 an trusted execution environment. All files and all communication is 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**. Violations of memory safety are the main cause of intrusions like those based on infamous Heartbleed attack[[7]](#footnote-8).
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[[8]](#footnote-9)*.
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 a scalability of their existing businesses without the risk of large hardware investments while protecting the IP and application data.

### 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.

Using SGX is, however, not easy. The **performance impact** can between x2 (sequential access) and x2000 (random memory access) slowdown. Since the operating system is not permitted to access the memory of an application, one cannot issue system calls from within secure enclaves. System calls are, however, necessary to communicate with other services and clients. A thread inside a secure enclave must therefore first copy all arguments of a system call to the outside, leave the enclave to perform a system call and then re-enter the enclave (this is a “**synchronous system call**”). This is expensive and hence, we have implemented an **exit-less asynchronous** system call interface that has about an order of magnitude higher system call throughput in comparison to synchronous system calls. This actually enables us to run some services with a higher throughput inside an enclave than outside of an enclave.

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 – slowdowns between x2 to x10 are typical. Using hardware properties of enclaves, we are actually able to reduce the slowdown to about 18% inside of enclaves.

**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, i.e., the client can be sure to get access to the newest versions of these applications with the latest security patches.

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

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

b) 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

c) all communication with the enclave is encrypted – not only all TCP connects but also *stdin*, *stdout* and *stderr* streams are encrypted.

We will provide companies with service contracts that gives customers 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**. We will provide a private repository for secure containers and managed nodes for secure containers. While the price for secure containers will be on par with Docker (currently, $7 per month for 5 repositories), we will charge more for nodes running secure containers. This will require initially about $150 monthly costs per node instead of $15 monthly per node. This price will, however, need to be adjusted based on real costs and the availability of other clouds offering SGX enabled machines.

**Secure Application Platform and programming language support**. To reach TRL7 and above, we need to gain experience in running a secure container platform and secure applications. Our objective is to port to real-world, existing services inside of secure containers within the SCP project. While the popular container images are mainly written in C and C++ which we already support. However, many modern applications are written in other popular languages like Java, Go, and C#. Within SCP, we will focus on support for **Go** and **C#**. We are aware that Java is very important language but a) the support of Java is difficult, and b) it looks like that within the SERECA H2020 project, RedHat might support the porting OpenJDK to secure enclaves[[9]](#footnote-10). We will focus on one hand on C# since many modern applications are written within C# and the Mono platform[[10]](#footnote-11) supports ahead of time (AOT) compilation of C# programs. This is important for secure enclaves since we want to ensure minimal binaries for performance and security reasons. JIT (just in time) compilers are typically very large and hence, we would like to avoid running a JIT compiler inside of an enclave. On the other hand, we will also support the software written in the GO language inside of enclaves. The Docker platform as well as some popular services like **Consul** are written in GO. The support of GO will permit us to run some critical service like a coordination service (i.e., Consul) as well as certification authorities (part of Docker swarm) inside of enclaves.

**Secure pilot applications**. Within the SCP project, our objective is to port the flagship application of EXUS (i.e., EST) and that of SYNC (i.e., StreamLog), respectively within secure containers. The reasons for moving these applications in secure containers are different. The flagship program of EXUS is EST[[11]](#footnote-12). This 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:

* Identify and treat credit risk early
* Perform efficient collections
* Manage legal proceedings and recoveries
* Gain detailed insight into portfolio evolution, collections strategies and resource efficiency

Currently, the product roadmap sees the transfer of **the software to the cloud** in order to facilitate a range of new features as well as a different business model. Clearly, the confidentiality as well as the integrity of the data processed by EST 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[[12]](#footnote-13). Within SCP, we ensure that all data accessible by the cloud provide is encrypted. EFS is written in C# and our pilot application to show the support for C# application running inside of secure containers.

The flagship application of SYNC is SteamLog[[13]](#footnote-14). 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. Already since November 2008, Italian law mandates that abuses by system administrators be detected, the data owners are to be notified and the 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.

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.

## Relation to the work programme

*Working together, partners with complementary backgrounds, knowledge and skills, and in new and established value-chains, can turn these ideas into sustainable innovative products, processes and services…*

SCP combines partners with complementary expertise and clearly identified contributions to create a unique and new value-chain: SIL provides secure container environment and secure container images, 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).

*Innovative products, processes and services … address societal challenges … highly competitive in global markets.*

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%[[14]](#footnote-15), surveys indicate a shift towards 59% considering cybersecurity as a competitive advantage within 3 years.

*Accelerate this commercialisation process by providing extended funding opportunities through an open and agile scheme nurturing bottom-up ideas from innovative constituencies across Europe.*

SCP implements a “go-to-market” scheme. To ensure early exposure and continuous involvement, SCP uses an agile development scheme to create a continuous online testing channel, and incorporates a complete knowledge and collaborative based environment and different incentives to attract both customers and IT Providers to collaborate.

*Supports projects undertaking innovation from demonstration stage to market uptake, including piloting, test-beds, systems validation in real world/working conditions, validation of business models.*

SCP will develop an innovative secure container platform that will be demonstrated and demonstrated in operative environments. This will become a market-ready platform by the end of the project. The pilots and the evaluation will permit us to evolve the current prototype in the direction required by the market.

*It targets relatively mature new technologies, concepts, processes and business models that need a last development step to reach the market and achieve wider deployment*.

SCP starts from an existing prototype and existing secure container images at TRL3 and will move these to TRL7. The detailed table is provided in Section 1.3.

*Proposals must relate to any field under "Leadership in enabling and industrial technologies" and/or to any of the specific objectives under the priority "Societal challenges".*

SCP focuses on improving cyber-security for SMEs, directly related to the *Secure Society Challenge* and more specifically to the specific aim *Cyber Security for SMEs, local public administration and Individuals.*

## Concept and approach

### 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 cryptographic hardware found in upcoming commodity CPUs—in particular, Intel SGX.[[15]](#footnote-16) 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”.

Current commercial products for SGX are so far limited. Microsoft supports secure enclaves within Windows but does not support paging – limiting enclaves to only about 90MB. Intel provides a SGX driver for Linux that supports paging. In this way, enclaves can be up to a size of 64GB. Paging introduces some overhead. In case, programs have good locality or mainly sequential accesses, overheads can be kept to a factor of x2. It is expected that the next generation of Xeon CPUs will have a much better support for enclaves, in particular, these enhancements will reduce the paging frequency and hence, the runtime overheads.

Intel supports 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. For new applications, this seems to be an acceptable approach. However, splitting existing applications in two parts (data+ code inside an enclave and data+code outside of the enclave) is a very difficult challenge. This partitioning introduces performance overheads for entering and leaving the enclave and hence, one wants to limit such enclave transitions. Even more difficult are the security challenges such a partitioning introduces since one defines a new interface inside an existing application that provides access to the data and code kept inside of an enclave. Such a reengineering existing applications has proved to be an extremely difficult endeavor since, for example, often classes would need to be split in two – to keep the security relevant fields of an object inside an enclave and the remaining data 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.

The secure container will run on top of operating systems. They are protected against attacks from/via the operating system (these are 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[[16]](#footnote-17). 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 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 does not fit inside about 90MB[[17]](#footnote-18). We will provide a mechanism (with 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 since 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.

### Strategy and approach

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

* **Ease of use**. SCP is based on well known concepts like Docker containers and images. Also a Docker infrastructure is usable. The main complexity of the SCP approach is hidden in the generation of secure container images which are made available via a **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. Integration with Docker swarm requires an **enterprise-level subscriptions.**
* **Transparency.** Enterprise-level subscriber can get access to all source code that runs inside of enclaves via an additional **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 have a free tier that includes

The two pilot applications allow us to integrate two flagship applications inside of secure containers. This facilitates us to learn …

## 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. No commercial offering is so far 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 also 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 customised language/runtime systems[[18]](#footnote-19) require the developer to adapt the application.

**SCP adopts a container-based approach using the Docker framework. Docker-based application containers are orders of magnitude smaller and less complex than full virtual machines, which will therefore serve as the interface between the user’s application in form of a micro-service and the underlying software and hardware stack. The 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 micro-service based applications because of the need for a lightweight mechanism to host the potentially large quantity of micro-services.**

Our existing implementation of secure containers uses Docker.

**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 and efficiency of containers with the security levels previously only achieved by air-gaped 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 version 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.**

### 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 SecureCloud extends beyond |
| The SERECA[[19]](#footnote-20) project focuses on secure reactive programming in public clouds with the help of SGX secure enclaves. | The focus of SCP is on selecting some of SERECA result to increase their TRL to ensure that they can commercially be exploited. The focus is on exploitation of standard applications investigated within SERECA as well as the system support developed within SERECA. |
| SecureCloud[[20]](#footnote-21) 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 commercially be exploited. |

# Impact

According to Cisco’s Global Cloud Index Forecast, more than 30% of the cloud workloads will be in public cloud data centres by 2018. They expect the workflows in clouds to nearly triple between 2013 and 2018, while the workload of traditional data centres 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.[[21]](#footnote-22) 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.[[22]](#footnote-23) 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 over the next 12 months starting on 2015.[[23]](#footnote-24) According to Ovum, by 2016, 75% of EMEA-based enterprises will be using IaaS with investments in private cloud computing showing the greater growth.[[24]](#footnote-25)

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[[25]](#footnote-26) 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 organisations 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 dependability-enhanced cloud technology, such as the one being developed by SecureCloud. In the following, we briefly comment on some of such drivers, and provide factual data about market forecasts for each of them.

The Infrastructure-as-a-Service market in Europe is expected to grow quickly over next few years. The main factor accelerating this growth rate is widely considered to be the comparable cost effectiveness. According to a forecast by International Data Corporation (IDC), worldwide spending on public infrastructure will reach $107 billion by 2017 having a compound annual growth rate (CAGR) of 23.5%, five times greater than that of the entire IT industry. Information technology research and advisory firm Gartner group forecasts similar results, predicting IaaS spending growth of 19% CAGR. Gartner’s research suggests cloud computing is fast becoming the bulk of new IT spending and should dominate by 2016. They predict that by 2016 private cloud will begin to give way to hybrid cloud with nearly half of large enterprise having hybrid cloud deployments by the end of 2017.

## Expected impacts

The outcomes of SecureCloud project will produce breakthrough solutions for cloud computing service providers with the current (insecure) cloud service composition as well as the user of such services. 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 SecureCloud research results to be deployed within 2 to 5 years after the project completion. It can be even shorter as cloud computing services are catalysts for sustainable developments in Europe. These deployments are associated with the need of organisations to share knowledge, resources and work towards common business goals.

In Europe, the possible set of shared resources between organizations should not be restricted to cloud storage or computing, but must include service elements as the building blocks of such services. The secure virtualized infrastructure of SecureCloud and its management solutions represent a fundamental opportunity in the European regulatory framework to strengthen the position of cloud computing providers delivering services. With strong business cases for more secure access of infrastructures from service developers and providers facilitated with programming environments supporting open and standard interfaces, SecureCloud will impact how developers design their next generation systems to be deployed on the Internet, and how companies offer new services.

With the results expected by SecureCloud, cloud service platforms enabled with secure enclaves 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 to lead the definition of new service platform technologies.

SecureCloud will develop novel technologies in cloud computing, addressing several challenges proposed in the Horizon 2020 Work Programme for Leadership in enabling and industrial technologies in Information and Communication Technologies, especially those listed in the coordinated call with Brazil H2020-EUB- 2015. In this section, we enumerate the expected impacts in the call and the contributions of SecureCloud addressing these impacts.

**Expected impact**: *Development of technologies integrating cloud and big data in terms of architecture, middleware and services.*

* **Contribution**: Advance state-of-the-art technologies for detailed QoS monitoring and enforcement.

The cloud elasticity can be nullified by the lack of suitable adaptation mechanisms. A middleware that offers detailed monitoring and highly responsive orchestration services that work seamlessly together will provide mechanisms for building both applications and platforms that can react quickly to a changing environment and, thus, can enforce specified Quality-of-Service metrics. This will be possible through an intelligent system that not only collects a rich set of metrics in a detailed fashion, but also processes the high-volume low-level data to generate meaningful actionable information.

* **Contribution**: In SecureCloud, we address dependability, confidentially and integrity by introducing micro-services that run inside of secure containers.

The micro-service abstraction allows a much wider adoption of cloud services compared to traditional IaaS offerings as customers can focus on data analytics and business logic leaving out the burden of maintaining explicitly an infrastructure in form of virtual machines to run services. In contrast to existing service offerings such as Amazon Lambda, the micro-services provided through SecureCloud are dependable and run in secure containers, thus increasing the trust of the user in the cloud provider and allowing a wider adoption of cloud technologies.

* **Contribution**: The implementation efforts taken in the SecureCloud platform will be contributed to the open-source OpenStack technology, hence increasing the customers trust in that technology.

The use of open-source technologies for cloud service offerings such as the SecureCloud platform allows a wider adoption of cloud technology as it increases transparency of the implementation for the underlying software stack, and provides trusted security when using secure micro-services due to their reliance on secure containers. Moreover, the use of open-source technologies allows a close collaboration with existing communities and provides a close feedback loop.

* **Contribution:** The consortium will develop the appropriate use cases for demonstration of SecureCloud platform capabilities to improve the competitive position of the European cloud sector on example of smart grid critical infrastructure.

The smart grid critical infrastructure is a target of different cyber attacks therefore the consortium will demonstrate that the SecureCloud platform can improve the assurance of computing techniques for Smart Grid applications.

* **Contribution**: Cloud data privacy by design.

SecureCloud combines secure processing with secure data storage developing cutting-edge techniques for data privacy by spreading stored data over multiple cloud providers. These capabilities are key for sensitive data, ranging from end-users' personal data, to personal sensor/location data and home smart metering. These new capabilities, developed as part of SecureCloud's WP4, provide a unique market offering for EU's SMEs to impact the Cloud security sector, which is set to increase its yearly investment from $9 billion in 2013 to $16 billion in 2016. This is also particularly interesting as the cost for lost/compromised personal data/record in 2013 amounted to an average of $145 per record, with companies in the United States losing the most per record for each data breach ($201 per record) followed by Germany ($195 per record). The total cost for data breaches amounted to around $300 million in 2013.[[26]](#footnote-27)

* **Contribution**: The smart grid critical infrastructure is a target of different cyber attacks therefore the consortium will demonstrate SecureCloud platform will improve the credibility of the computing technique for Smart Grid applications.

The consortium will develop the appropriate use cases for demonstration of SecureCloud’s platform capabilities to improve the competitive position of the European and Brazilian cloud sector on example of smart grid critical infrastructure.

* **Contribution**: The consortium will implement a validation process based on a dedicated environment supported by the Israel Electrical Corporation. This environment allows to develop and to test tools and methodologies over mirrored critical infrastructures, assessing risk and simulating real scenarios.

IEC will customize its validation environment for specific requirements of SecureCloud project. The project partners will use the environment for system development and integration, and for validation cyber attacks.

* **Contribution**: The consortium will develop and validate a platform for smart metering applications focusing on the security requirements necessary for smart metering sector of Brazilian energy sector.

SecureCloud platform will be created and validated to enable both the storage of critical data and specific software for smart metering and fraud detection systems, according to the requirements used by Brazilian utilities. All those solutions will be validated using real smart metering data acquired by Lactec on its Smart Grid pilot and in Brazilian utilities systems.

**Expected impact**: *Facilitate the development of cloud enabled applications through robust standardized global technologies.*

* **Contribution**: Design and implement services that manage secure containers in an open-source middleware.

Using a service-oriented approach, we will provide generic services that build a foundation for implementing cloud-based platforms for secure applications. Using these services, secure resources will be managed at the same level of abstraction as typical cloud infrastructure resources, such as object storage, VMs and volumes. This will enable cloud providers to use secure resources efficiently and cloud customers to build cost-effective secure applications.

* **Contribution**: Identify and propose patterns for cloud-based big data applications that are quality-of-service, privacy, and security aware.

The SecureCloud project will develop a rich set of applications that combine security, privacy and QoS at different levels. Our diverse and experienced partnership will ensure that these applications are effective and practical. It can thus identify patterns and offer templates for the implementation of other applications that should observe security, privacy and QoS, even in other domains.

* **Contribution**: Data privacy in cloud services has been a matter of debate in recent years. There is a lack of trust in cloud providers since they are able to read personal data (as stated in various Terms of Service), share it with governmental agencies, or be breached by malicious attackers. In SecureCloud, we will address the problem of data privacy by using cutting-edge technology allowing us to store data with different levels of protection and in multiple locations.

SecureCloud will allow cloud developers to manage data privacy of stored data by design and using different levels of security for the data, including the distribution of data amongst multiple cloud providers. These capabilities can be integrated seamlessly with standard technologies for communicating with existing Cloud providers. These strategies and capabilities are key due to (i) the increasing legal constraints for storing data within the borders of EU countries, and (ii) the fact that European countries have been found to receive four times more cyber attacks than the US.[[27]](#footnote-28)

* **Contribution**: SecureCloud will develop a validation system for demonstration and evaluation of cloud-based services in federated, heterogeneous and multi-layered cloud environments, of the dynamic provisioning of interoperable applications and services, as well as technologies integrating cloud and big data in terms of architecture, middleware and services, applied to a smart metering application.

The validation as developed in SecureCloud will establish a new level of secure technology for the cloud and will demonstrate how this technology can be adapted for faster adoption by critical applications similar to those of the smart grid.

**Expected impact*:*** *Joint contributions to International Standardisation and/or Forum activities*

* **Contribution:** The project will closely monitor the main standards and/or standardization activities that are relevant for cloud computing security. The work of the main standardization bodies, technical committees, and forums will be followed closely, to ensure that results be used in SecureCloud.

The indications provided by the by the selected standardization bodies, technical committees, and forums will be promoted via the participants’ network of connections, to form a triple-helix collaboration commitment among leading companies, research centres, and universities and to cluster with relevant funded projects in Europe, in alignment with the aims of Horizon 2020.

* **Contribution:** Some of the partners of the consortium have been active contributors for several years to standardization bodies that are of specific interest to the project.

Members of SyncLab are actively involved in and willing to contribute to ETSI TISPAN WG6 and some IETF Working Groups, as well as ETSI Cloud Technical Committee and IETF initiatives on cloud computing standardization.

### Alignment with EU strategies and policies

SecureCloud 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, SecureCloud 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

## Measures to maximise impact

SecureCloud 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.

### Dissemination and exploitation of results

Dissemination and preparation of exploitation of the project results are issues addressed within WP6. Dissemination activity is considered any task that aims at disseminating the results of the project, promoting the SecureCloud concept, increasing the visibility of the project and supporting the exploitation of the results achieved. Dissemination and exploitation measures that the Consortium has planned address the full range of potential users and uses. The approach to innovation is comprehensive, and it is tailored to the specific technical, market and organisational issues addressed by the project. In order to achieve these goals, massive dissemination and exploitation activities have been planned, that will span the entire duration of the project. For better performance, activities will be organized in several subtasks, and in particular: Raising User Participation and Awareness; Web-based dissemination and Social networks (e.g. Facebook, Twitter, Vimeo, YouTube); Printed dissemination material; Workshops and Conferences; Publications; Radio interviews; Exploitation planning; Clustering with other projects; Market analysis; Exploitation plan; Coaching; Training and knowledge transfer; Production of training material; Organization of training events.

### Training

The academic partners already offer—also in cooperation with other outstanding European universities—Masters and PhD school programs that are closely related to the research that will be done in SecureCloud, e.g. the International Master's Program in Distributed Systems Engineering (TUD). In case of funding, a PhD school will be jointly organized by the academic partners, featuring and industry session by the industrial partners of the SecureCloud project.

.

### Initial dissemination plans

TUD, as the coordinator of SecureCloud, 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 SecureCloud. TUD will promote SecureCloud’s outcome in the following ways:

.

### Expected exploitable results

Usage of cloud offerings independently of the deployment and the service model is proven a very profitable investment for SMEs and large companies with multiple benefits regarding ROI (Return on Investment), since the deployment cost for the service is reduced. Main concerns are associated with the data migration and user mobility and how the confidentiality and privacy is preserved.

In order to ensure maximal exploitation of project’s results SecureCloud has adopted a stepwise approach:

* Step 1: Technology review update (not SOTA analysis) of all relevant background including cloud security as well as technologies and techniques for fault and intrusion detection, auditing facilities and secure communication channels taking into account international and national directives and European strategies in order to carry out complementary primary research where required.
* Step 2: Analysis of complementary and competitive services and relevant shortcomings that need urgently to be addressed at a global level in order to pave the way of cloud adoption by industry, as well as identification of emerging best practice across several domains that addressed by the project and involving huge data processing as well as the wider involved public and private domain internationally.
* Step 3: Setting up of deployment scenarios, market and business models for individual exploitation and joint exploitation, specifying collaboration roles, costs and revenue flows, specifying as well necessary guidelines that need to apply in order to make such scenarios feasible;
* Step 4: Validation of business models and deployment scenarios within the feasibility analysis with the help of the partners’ complementary expertise and assessment of the effectiveness of the SecureCloud approach to provide a leap forward in the area of cloud security in different domains.
* Step 5: Organization, planning and execution of wide impact dissemination activities to create full awareness of SecureCloud activities, its approach and results in the academic community, among public authorities, service and solution providers as well as contributing to the EU strategic roadmap for the fast adoption and usage of cloud security modules; establishing contact with key third parties for exploitation.
* Step 6: Regular review, revision and refinement of partner-specific exploitation plans and joint and collaborative business plans in the light of interim project results; formalization of service level and other appropriate agreements for joint exploitation among partners and third parties;

The SecureCloud consortium under the auspices of the coordinator and with joint exploitation activities organized and coordinated by Sync Lab aims at promoting novel solutions and products in several market places and segments such as Healthcare, telecommunication, gaming and authoring, public protection, security and the banking sector.

### Preliminary exploitation plans

Industry and SMEs: All industry partners’ expertise in the area of security in cloud platforms will increase due to international collaboration with major players and academic partners, and they will achieve competitive advantages to reinforce their presence in national and international markets, and enter new markets as well.

### Research data management plan

##### Policy for Data Management

SECURECLOUD 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 (D6.2), and two updates are planned at month 24 and 36. 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.

##### 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-) anonymisation techniques. Anonymised 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 SECURECLOUD 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, anonymised data that demonstrate the use of the system can be made available given that all legal requirements are fulfilled.

##### 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, on a RAID device. The data will be stored, archived, and preserved for the duration set by the legal framework.

### 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, several of the partners have participated in previous EU funded projects, exhibiting high involvement in communication initiatives.

# Implementation

## Work plan — Work packages, deliverables and milestones

### 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 – pilots – 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 22 testing sessions focused on users. In addition to the 22 sessions, a continuous trial channel will be opened, linked to the 2 weeks sprint and to a group of beta-testers created 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 two large organisation pilots will focus on using the two flagship applications in the context of a large organisation.

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 organised by the project.

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

(to do – replace the following fig ... in the works)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP1** | **Requirements, specification, design of the SecureCloud platform** |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T1.1 | Definition of use cases and requirements |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.2 | Design and specification |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.3 | Infrastructure for continuous integration |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.4 | Continuous assessment |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP2** | **Infrastructure services to enable secure, QoS-aware applications** |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  | ■ |  |  |  |  |  |  |
| T2.1 | Evaluation of technology trade-offs |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.2 | Management and lifecycle of secure containers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.3 | Trust management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.4 | QoS monitoring and enforcement |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP3** | **Dependable Micro-services for the Cloud** |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T3.1 | Framework for restartable secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.2 | Set of reusable secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.3 | Dependability management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.4 | Templated programming model for secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP4** | **Secure distributed big data application with micro-services** |  |  |  |  |  |  |  |  | ■ |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T4.1 | Secure distributed communication mechanisms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.2 | Secure distributed data management and storage |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.3 | Distributed scheduling mechanisms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.4 | Secure map/reduce computation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP5** | **Demonstration and Evaluation** |  |  | ■ |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T5.1 | Data preparation for validation of developed algorithms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.2 | Development of monitoring and control applications for smart grids |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.3 | Test and validation of secure applications for privacy-sensitive data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.4 | Tests and validation of applications with strict QoS requirements |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP6** | **Dissemination, Exploitation and Communication** |  |  | ■ |  |  | ■ |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T6.1 | Dissemination of project results, and clustering activities |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.2 | Market Analysis and Business Plan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.3 | Project Public Web site |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.4 | Open Standardization Activities |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP7** | **Project Management** |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T7.1 | Project coordination |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T7.2 | Administrative, financial and legal management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T7.3 | Internal website and communication Tools |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Milestones** | |  |  |  |  |  |  |  |  | ▲ |  |  |  | ▲ |  |  |  |  | ▲ |  |  |  |  |  |  | ▲ |  |  |  |  |  |  |  | ▲ |  |  |  |

■ Deliverable ▲ Milestone

Table 3.1‑1: Gantt Chart

### 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** | **15** | | 2 | 2 | **17** | |

|  |
| --- |
| **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, organisation 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 | **28** | |

|  |
| --- |
| **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 | **Total** | |
| **Name of participant** | **SIL** | | SYNC | EXUS |
| **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 SreamLog** *(Months:* ***M6-M30*** */ Partners:* ***SYNC (task leader), all)***  The objective of this task is to adapt and extend the SteamLog 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: M21, 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** | | | | M1 |
| **WP title** | Piloting | | | | | |
| **Participant number** | **1** | | 2 | 3 | **Total** | |
| **Name of participant** | **SIL** | | SYNC | EXUS |
| **PMs** | **30** | | 20 | 20 | **70** | |

|  |
| --- |
| **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: M1-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. The planning will also include the validation of the online support elaborated in task 5.3.  ***T 4.2: SCP platform pilot execution and validation (Months: M8-M30 / Partners: SIL (task leader), SYNC)***  This task implements 22 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 SteamLog, 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 adapatation. |

|  |
| --- |
| **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.  ***D4.4, D4.5 (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 | **Total** | |
| **Name of participant** | **SIL** | | SYNC | EXUS |
| **PMs** | **22** | | 11 | 11 | **44** | |

|  |
| --- |
| **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 organisations 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-M15 /*** *Partners****: SIL (task leader), all)***  This task defines and organises the open call(s) to identify SMEs who will participate to the two piloting iterations and user mock-up testing phase. The approach is to select 5 to 10 SMEs in the first call, organised at M2. The selection criteria include profile of SME in terms of level of expertise in IT, coverage of activity sector, maturity level in managing risks, size and diversity of assets to protect. The task foresees a first call at M2; depending on the outcome of the call, a second call could be organised (indicated in the Gantt chart) at M13. The decision to organise a second call will be taken within task 1.2 at M12, following the finalisation of the first set of piloting sessions. The decision will be based on whether it is preferable to include additional SMEs to increase the diversity of coverage, or to run a second set of piloting sessions involving the start-up phase of deploying CRiSP etc.  ***T5.5:******Exploitation channels and road-show*** *(Months:* ***M13-M24*** */ 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.  ***T5.6: Communication activities*** *(Months:* ***M7-M24*** */ 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: CYS, 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 (Other): SME Call (Editor: ENG, Delivered: M2, M13 (optional), Related task: T5.2)***  **This deliverable is the open call to identify the SMEs who participates to the mock up testing and to the piloting activities. The deliverable may take different forms, depending on the channels used to announce the open call. A second (optional) version of the deliverable (D5.2b) could be issued at M13, as detailed in task 5.2 above.**  ***D5.3 (Report): CRiSP User Group (Editor: ENG, Delivered: M24, Related task: T5.3)***  **This deliverable reports about the activities and interactions of the CRiSP user group during the project lifetime.**  ***D5.4 (Report, Other): CRiSP Training and Support (Editor: CINI, Delivered: M10, M24 Related task: T5.4)***  **This deliverable contains the online training and support facilities for the CRiSP solution. The first release of the deliverable will contains the design of the facilities, while the second one will contains a revision based on the experience gained during the development of the project.**  ***D5.5, D5.6 (Report): Communication activities (Editor: ENG, Delivered: M12, M24 Related tasks: T5.5, T5.6)***  **This deliverable reports all the communication activities carried out, including the exploitation channels and road-show, conferences, publications etc. It also analyses the KPIs linked to the go-to-market strategy and updates the strategy elaborated in T5.1 as necessary** |

### List of Work Packages

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **WP** | **WP title** | **Lead no.** | **Lead participant** | **Person months** | **Start month** | **End month** |
| WP1 | Bla bla | 1 | TUD | 63 | 1 | 36 |
| WP2 | Infrastructure services to enable secure, QoS-aware applications | 9 | UFCG | 101 | 1 | 30 |
| WP3 | Dependable Micro-services for the Cloud | 2 | IMP | 58 | 1 | 36 |
| WP4 | Secure distributed big data application with micro-services | 3 | UNINE | 79 | 1 | 36 |
| WP5 | Demonstration and Evaluation | 8 | LACTEC | 185 | 1 | 36 |
|  |  |  |  | 541 |  |  |

Table 3.1‑2: List of Work Packages

### List of Deliverables

| **Del. no.** | **Deliverable name** | **WP no.** | **Lead part.** | **Type** | **Dissem.**  **level** | **Delivery month** |
| --- | --- | --- | --- | --- | --- | --- |
| D1.1 | Requirements & Architecture specification – initial version | 1 | TUD | R | PU | 9 |
| D1.2 | Requirements & Architecture specification – intermediate version | 1 | TUD | R | PU | 21 |
| D1.3 | Requirements & Architecture specification – final version | 1 | TUD | R | PU | 36 |
| D2.1 | Analysis of existing technologies | 2 | TUD | R | PU | 12 |
| D2.2 | Prototype services for basic management of secure resources | 2 | UFCG | DEM | CO | 24 |
| D2.3 | Services for trust management for secure resources | 2 | UFCG | OTHER | PU | 30 |
| D2.4 | Monitoring and orchestration services for large, high-responsive applications | 2 | UFCG | DEM | PU | 30 |
| D3.1 | Specification and implementation of the micro-service framework and API | 3 | IMP | DEM | PU | 12 |
| D3.2 | Specification and implementation of reusable secure micro-services | 3 | IMP | DEM | PU | 24 |
| D3.3 | Description of dependability mechanism used by the micro-service framework | 3 | TUD | R | PU | 36 |
| D3.4 | Description of programming model for new micro-services | 3 | IMP | R | PU | 36 |
| D4.1 | Specification and design of the micro-services for distributed big data applications | 4 | UniNE | R | PU | 9 |
| D4.2 | Preliminary implementation of the communication and storage mechanisms | 4 | CC | DEM | PU | 12 |
| D4.3 | First implementation of the micro-services for distributed big data applications | 4 | UniNE | DEM | PU | 24 |
| D4.4 | Integrated implementation of the micro-services for distributed big data applications | 4 | UniNE | R | PU | 36 |
| D5.1 | Database for the testbed that will run smart grid application to the cloud | 5 | LACTEC | OTHER | CO | 3 |
| D5.2 | Cloud-native applications for billing, fraud detection, energy balance, energy delivering and fault detection | 5 | LACTEC | OTHER | PU | 14 |
| D5.3 | Demonstrator for the end-to-end secure and privacy-friendly application for smart meter data | 5 | UTFPR | R | PU | 24 |
| D5.4 | Demonstrator for strict-QoS application with realistic workloads running in a secure cloud | 5 | UFCG | DEM | PU | 36 |
| D6.1 | Project web site | 6 | SYNC | R | PU | 3 |
| D6.2 | Data Management Plan | 6 | SYNC | R | PU | 6 |
| D6.3 | Project dissemination and clustering activities report (3 versions) | 6 | SYNC | R | PU | 12,24,36 |
| D6.4 | Project exploitation and use plan (2 versions) | 6 | SYNC | R | PU | 24,36 |
| D6.5 | Standardization activities | 6 | SYNC | R | PU | 36 |
| D6.6 | Periodic research newsletter (3 versions) | 6 | SYNC | R | PU | 12,24,36 |
| D7.1 | Project Management Tools | 7 | TUD | R | CO | 3 |
| D7.2 | First Periodic Report | 7 | TUD | R | CO | 18 |
| D7.3 | Final Periodic Report | 7 | TUD | R | CO | 36 |
| D7.4 | Final Report | 7 | TUD | R | CO | 36 |

Table 3.1‑3: List of Deliverables

## Management structure and procedures

### ../../../../../Dropbox%20(Personal)/Screenshots/Screenshot%202016-03-11%2007.10.13.pOrganisational 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 optimising 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 abovehas 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 organisational structure has been agreed to optimise planning, monitoring and coordination of SCP project activities, tasks performance, reporting and accountability.

#### Key Roles and Committees

The project will be implemented under the executive management of the **Project Coordinator (PC),** whowill 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 synchronisation 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**, thehighest 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** |
| MS1 | System requirements complete | WP2 | M6 | D2.3 available |
| MS2 | CSP platform released for 1st pilots | WP3 | M12 | First platform prototype available |
| MS3 | CSP platform released for 2nd pilots | WP3 | M17 | Second platform prototype available |
| MS4 | CSP platform final release | WP3  WP5 | M30  M22 | Final version of CSP available  Online training facility operational |
| MS1 | System requirements complete | WP2 | M6 | D2.3 available |

Table 3.2‑1: Scheduling of milestones

#### Appropriateness of the Organisational Structure

SCP will deploy best practice innovation management methods to realise an extensible and flexible product closely oriented to market needs. The project will be closely connected with users through 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, 3 and 4. To ensure that relevant opportunities are identified and responded to, all consortium members will contribute to exploitation meetings (in coincidence with ordinary TMC meetings) with a horizon scanning report. The resulting horizon scanning capability will be important in informing development decisions throughout the project and will also draw on inputs from the users and the markets.

### Risk Management

The CSP 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 an exploitation of the SCP platform by SIL and the pilot applications by EXUS and SYNC will be performed. 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 CSP obsolete before reaching the market | WP5 | SCP is positioned in a huge potential market – in which there is room for a number of players. |

## Consortium as a Whole

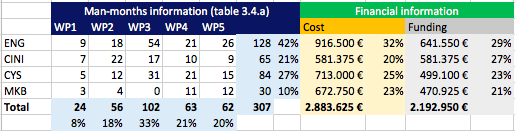
The SCP consortium builds on complementarity and full coverage, namely:

* the consortium provides the *full coverage of expertise and solutions to deliver SCP*
* 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 CRiSP, *prototypes have been already evaluated at least at TRL-3* level
* 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

## Resources to be committed

Resources are well balanced, with 41% of the efforts dedicated to piloting and exploitation (WP4+WP5), and 51% 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.



Three partners have “other costs” close lower than 15%. The other costs are detailed as follows:

ADD TABLE

1. See https://dockerhub.com [↑](#footnote-ref-2)
2. Of course, the security of the hypervisor, operating system and the cloud must not be neglected since successful attacks can lead to the unavailability of hosts and hence, to the unavailability of some application components. [↑](#footnote-ref-3)
3. **SCONE: Secure Linux Containers with Intel SGX** (Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, André Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Daniel O'Keeffe, Mark L Stillwell, David Goltzsche, Dave Eyers, Rüdiger Kapitza, Peter Pietzuch, Christof Fetzer), USENIX, 2016. [↑](#footnote-ref-4)
4. http://www.t-mobile.com/landing/experian-data-breach.html [↑](#footnote-ref-5)
5. https://software.intel.com/en-us/sgx [↑](#footnote-ref-6)
6. http://www.gartner.com/newsroom/id/3188817 [↑](#footnote-ref-7)
7. https://en.wikipedia.org/wiki/Heartbleed [↑](#footnote-ref-8)
8. see https://hub.docker.com/explore/?page=1 [↑](#footnote-ref-9)
9. Within the SERECA project, there is already support for JamVM an small Java virtual machine. Which would be out backup in case OpenJDK will not be supported after all. [↑](#footnote-ref-10)
10. https://www.mono-project.com [↑](#footnote-ref-11)
11. http://www.exus.co.uk/en/products/debt-collection-software-suite [↑](#footnote-ref-12)
12. http://www.zdnet.com/article/us-strikes-back-in-microsoft-email-warrant-case/ [↑](#footnote-ref-13)
13. http://www.synclab.it/prodotti/streamlog/ [↑](#footnote-ref-14)
14. 2015- Global Megatrends in cyber security , Ponemon institute, published 02/2015 [↑](#footnote-ref-15)
15. 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. [↑](#footnote-ref-16)
16. http://www.theregister.co.uk/2014/04/09/heartbleed\_explained/ [↑](#footnote-ref-17)
17. this is the usable size of the EPC (extended page cache) of current generation SGX implementations. [↑](#footnote-ref-18)
18. http://zerovm.org/ and http://zerg.erlangonxen.org/ [↑](#footnote-ref-19)
19. http://www.serecaproject.eu [↑](#footnote-ref-20)
20. https://www.securecloudproject.eu/ [↑](#footnote-ref-21)
21. 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 [↑](#footnote-ref-22)
22. http://news.investors.com/technology/011615-735080-amazon-aws-leads-in-cloud-msft-googl-crm-rising.htm [↑](#footnote-ref-23)
23. 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 [↑](#footnote-ref-24)
24. http://www.rackspace.co.uk/sites/default/files/UnlockedNov2014\_TheRoleOfCloudInITModernisation\_Ovum.pdf [↑](#footnote-ref-25)
25. http://www.skyhighnetworks.com/cloud-report/ [↑](#footnote-ref-26)
26. 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013. [↑](#footnote-ref-27)
27. Alert Logic CLOUD SECURITY REPORT – SPRING 2014. [↑](#footnote-ref-28)