MUlti-cloud Secure Applications

Deliverable title	Deliverable ID: D6.5
	Preparation date: 30/09/2015
Networking Plan	Editor/Lead beneficiary (name/partner): Valentina Casola / CeRICT Massimiliano Rak / CeRICT
	Internally reviewed by (name/partner): Stefan Spahr / LSY Antonio M. Ortiz / MI

Abstract:

This deliverable aims at illustrating the MUSA networking plan. This plan details the specific networking activities with both internal and external actors to MUSA project.
The internal networking activity aims to explore collaborations and knowledge exchange among MUSA partners and individuals, while the external networking activity aims to link the project to the community of stakeholders interested in the MUSA results, as well as to create synergies with other ICT projects under the same EU-ICT objective, increasing the impact of the ICT initiative.

Dissemination level		
PU	Public	X
CO	Confidential, only for members of the consortium and the Commission Services	

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 644429

MUSA consortium

	Fundación Tecnalia Research & Innovation (TECNALIA, Spain) www.tecnalia.com/en	**Project manager:** Erkuden Rios erkuden.rios@tecnalia.com +34 664 100 348
	Centro Regionale Information e Communication Technology (CER ICT, Italy)	Contact: Massimiliano Rak massimiliano.rak@unina2.it
	CA Technologies Development Spain SAU (CA, Spain)	Contact: Victor Muntes Victor.Muntes@ca.com
	Montimage (MI, France)	Contact: Edgardo Montes de Oca edgardo.montesdeoca@montimage.com
	AIMES Grid Services (AIMES, UK)	Contact: Prof Dennis Kehoe dennis.kehoe@aimes.net
	Lufthansa Systems (LSY, Germany)	Contact: Dirk Muthig dirk.muthig@lhsystems.com
	TTY-säätiö (TUT, Finland)	Contact: José Luis Martínez Lastra jose.lastra@tut.fi

Table of contents

List of figures

List of tables

Executive summary

The activities reported in this deliverable are related to Task 6.3 *Networking with external initiatives* in Work Package 6 (WP6) *Dissemination and communication* whose main objective is to maximize the impact of the MUSA project[1] by the definition of specific dissemination, communication and networking activities to exploit synergies for cooperation with targeted communities, stakeholders, dedicated Working Groups and related ICT projects that may be interested in the MUSA results from different points of view: research, scientific, commercial, industrial.
This deliverable wants to design the strategies and related plan of activities to build a professional network made of institutions, organizations and other actors interested in MUSA results; it is directly connected to the D6.2 *Dissemination Strategy* and D6.4 *Communication Plan* where overall dissemination and communication plans have been presented.

In order to make the strategy effective, the characterization of the target communities is very relevant. We ran this activity with a two-level analysis: (i) internal network and (ii) external network, i.e. internal and external with respect to MUSA project Consortium members. The corresponding plans have been delivered to strengthen the MUSA internal and external network: an internal networking plan that mainly involves each participant of the MUSA project and an external networking plan, including all the connections that MUSA project will create with other organizations.

1 Introduction

1.1 Objective of this document

The building of the MUSA Community network is a crucial activity to maximize the impact of the project; this is part of the Dissemination and Communication activities in Work Package 6.

The main goal of this deliverable is to define and develop a strategy that aims to build a strong network of actors interested in the project results and that can get a reciprocal advantage of being connected to MUSA. The network will help to optimize the project activity and to strengthen the commercial use of the project results during the project life cycle and after the project end. In particular we propose a strategy, articulated in two levels that respectively focus on the building of a so called "internal network", to facilitate and promote the networking among all MUSA partners to increase the value of specific skills, and of an "external network" to exploit synergies with other relevant EU initiatives as, for example, thematic working groups and other ICT-related projects.

In fact, the researchers involved in the consortium are the crucial point of the MUSA network. They represent the first nucleus that gets the opportunity to be part of an international network to strengthen the scientific reputation through the empowerment of knowledge and the increasing of the scientific production. In order to get these objectives the plan of networking activities is the document that describes actors involved, that identifies the position of the actors involved in the network and designs the strategies to get specific outcomes.

The specific activities, including the working groups and the clusters that this project will participate in, will be presented in the next sections; they strictly complement the activities presented in other deliverables (namely D6.2 and D6.4) for communication and dissemination activities. The plans and the activities here reported have to be considered as "live" documents, they will be periodically updated and improved in order to maximize the impact that the MUSA results can have on the scientific and industrial communities.

1.2 Structure of this document

This document is structured as follows:

- Section 1, after an introduction to the document, presents the relationship among this deliverable and other deliverables in MUSA and the main contributors to this deliverable.
- Section 2 overviews the networking strategy, by describing first of all the two network levels and, secondly the rationale behind the community building and networking approach.
- Section 3 overviews the internal networking strategy through the identification of three factors: researchers involved (Who), internal networking activities (What) and networking opportunities (How).
- Finally, Section 4 overviews the external networking strategy through the identification of external organizations already connected with MUSA partners (Who), the planning of external networking activities in combination with the current dissemination strategy (What) and networking opportunities (How). In particular, it presents an overview of possible collaborations with relevant research projects and working groups, as well as it defines a dedicated strategy for the involvement of industrial organizations.

1.3 Relationships with other deliverables

This deliverable, as the others in WP6, is strictly related to all Work Packages of the MUSA project as its goal is to maximize the impacts that the project results may have on both the academic and industrial communities by defining proper strategies for the building of a professional network of actors interested in the MUSA project results.

In particular, it is strictly related to activities and related deliverables of Work Package 6 (deliverables D6.2 *Dissemination Strategy*, D6.3 *Data Management Plan* and D6.4 *Communication Plan*) whose goals are to plan the proper dissemination, communication and networking plans and ensure that relevant communities will be located and reached out during the whole project lifecycle (from requirement analysis to development and exploitation).

Figure 1 describes the existing relationships between the dissemination and the networking activities respect to the project outputs. As illustrated, on one side, the dissemination activities are focused on defining a communication, social and dissemination strategy and identifying different communities and stakeholders (scientific, commercial, general public) to which project results will be targeted (deliverables D6.1, D6.2 and D6.4). On the other side, the Task T6.3 is focused on the Networking strategy where a specific plan is designed in order to empower the connections between MUSA partners and foster a close collaboration with projects related to MUSA; to create the condition to build a specific community of stakeholders, interested in the exploitation of project results (deliverable D6.4).

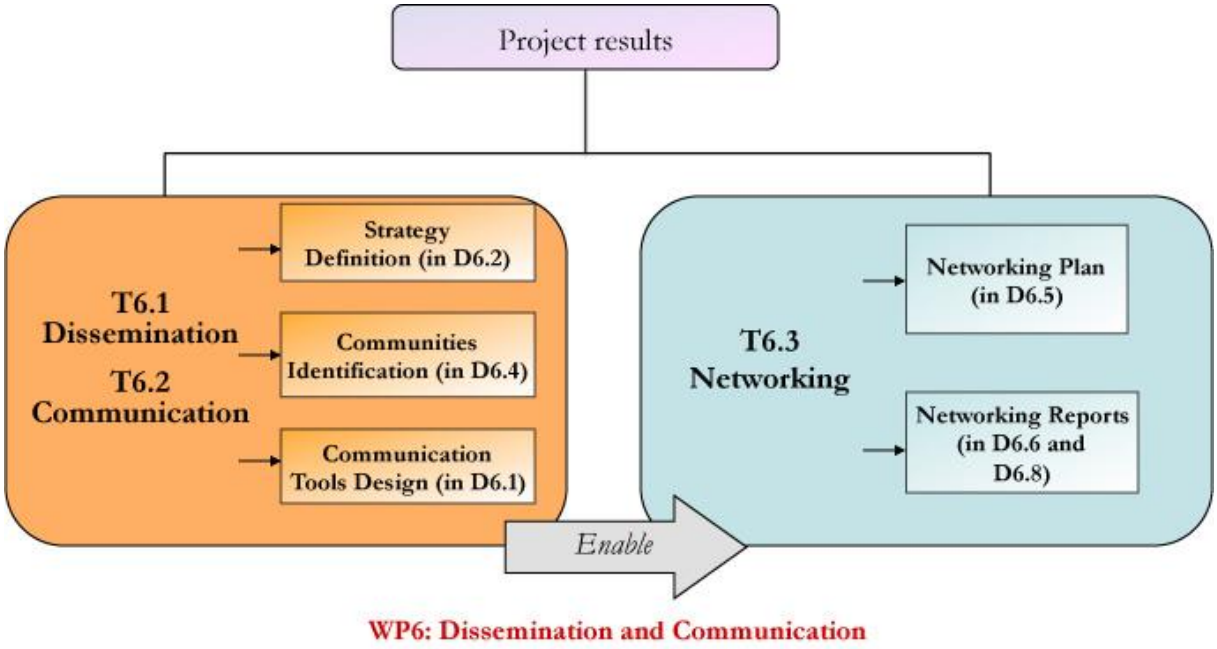

Figure 1: Relationships among MUSA Dissemination, Communication and Networking tasks

The networking activities and plans will be reported at the end of each reporting period respectively in D6.6 *Dissemination, communication and networking report* – intermediate report (M18) and in D6.8 *Final dissemination, communication, and networking report* – final report (M36), that will periodically report the status of all dissemination and networking activities. In addition, possible plan updates will be reported by the consortium in order to ensure the effectiveness of the plans.

1.4 Contributors

All the partners contributing to Task T6.3 have collaborated in this deliverable: CERICT (Leader), TECNALIA, CA, MI, AIMES, LSY, TUT.

1.5 Revision history

Version	Date issued	Author	Organisation	Description
0.1	15/04/2015	Valentina Casola	CeRICT	TOC proposed

Version	Date issued	Author	Organisation	Description
0.2	7/09/2015	Valentina Casola	CeRICT	Final proposed
0.3	25/09/2015	Valentina Casola	CeRICT	Final revised
0.4	29/09/2015	Marisa Escalante	TECNALIA	Improvement suggestions to Final revised
0.5	30/09/2015	Valentina Casola	CeRICT	Final released proposal
1.0	30/09/2015	Erkuden Rios	TECNALIA	Final released

2 Rationale for the networking strategy

This section describes the rationale behind the definition of the MUSA project network, aimed to empowering the synergies between MUSA and the existing projects and increasing the impact of project results respect to other ICT initiatives.

The networking is inspired by the following goals:

1. Optimizing the internal relations between partners, in order to disclose the embedded knowledge [3], connected to the practical and personal experience of each researcher;
2. Maximizing the impact of the project results, spreading the benefit to its partners as well;
3. Making the project results available to the ICT scientific community in the European Research Area.
4. Strengthening the relationship and create collaboration and business opportunities with stakeholders interested in the MUSA developments and results.

These are in line with EU directives. In fact, following EU Commission holistic approach, that involves Research and Innovation (R&I) to improve the development of each region (mainly reflected through the Smart Specialisation Strategy) [4] and provides clear impact on competitiveness, job creation and growth, the building of the MUSA community wants to sustain the European Territorial Cooperation Programs.

As illustrated in Figure 2, the EU strategy for growth is essentially based on H2020 and Cohesion Policy [5] that aim at achieving economic growth and prosperity by enabling regions to focus their strengths. The link between these pillars is the definition of Smart Specialization Strategy, designed to promote the efficient and effective use of public investment in research.

Figure 2: European synergic strategies for economic growth

The MUSA network will work to give its contribution to the creation of more equal conditions in all the European Countries thanks to its innovative results and technological frameworks in the field of Cloud Computing.

In particular, as pointed out in the project proposal, the MUSA networking will support the diffusion of its results, encouraging the *Digital Agenda flagship's* [6] Digital Single Market (pillar I), benefit greater interoperability (pillar II) and boost Internet trust and security (pillar III).

In line with the EU Data protection Reform [7] and the recently approved NIS Directive [8][9] MUSA will help European citizens consuming multi-cloud applications that really respect their data protection needs.

The definition of the MUSA community is crucial to spread the innovation of project results. In order to maximize the impact of the project, the internal partners of MUSA will cooperate to facilitate the

knowledge exchange and to share the connections that they have already activated in advance. The overall strategy is made of two different levels: (i) internal network and (ii) external network.

For this purpose, the MUSA network will be managed by following these actions:

- **Boosting the internal network**. For this aim, it is crucial to first identify the researchers /scientists involved in the project, then to involve different partners in common activities and encourage researchers exchange. At the same time, it is important the recognition of ICT projects run by each partner in previous experiences (see section 3 for details).
- **Building the external network**, through the identification of key actors, interested in the project results. In strong collaboration with dissemination WP, the project will be able to attract stakeholders, researchers and ICT scientists spreading the project results through a MUSA open source platform (see section 4 for details).

The building of the MUSA network starts from the empowerment of the internal connections between partners to build a wider network. MUSA networking strategy will consider each partner as first main knots of the network that will be enlarged as reported in Figure 3. In particular, the project networking aims to enrich the heritage of the previous project experiences made by each partner and give value to the existing relations that each partners has already activated carrying out its activity, in its own research field. From a macro point of view, MUSA involves three partners belonging to the Research community (Tecnalia, CERICT and TUT) and four partners from the Business community (CA Technologies, Montimage, AIMES, and Lufthansa Systems). The networking strategy will be focused on analysing the connections that each member has already developed through other project experiences.

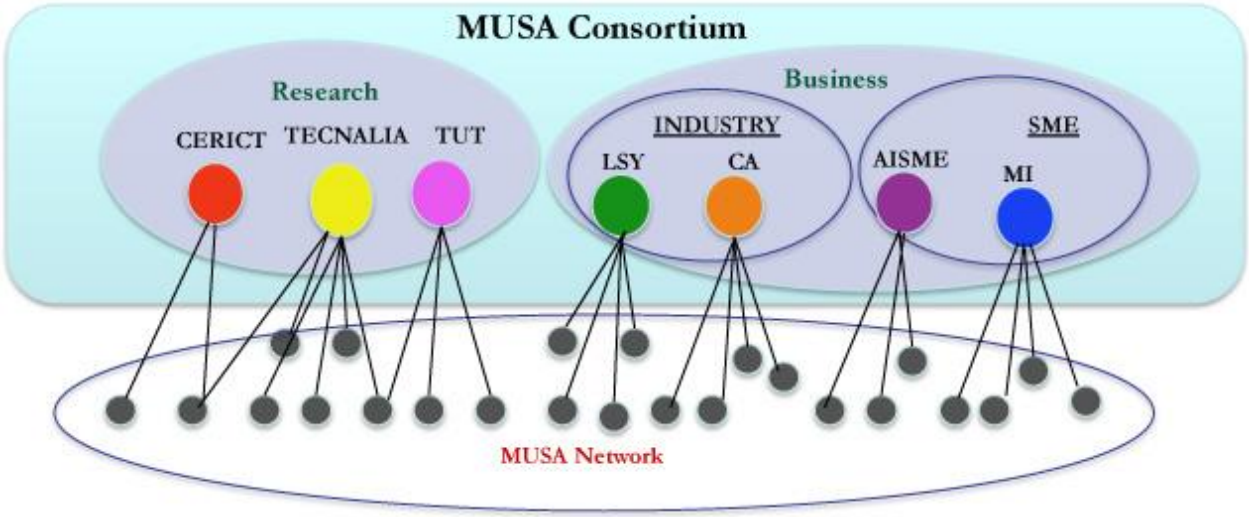

Figure 3: MUSA networks levels

In particular, the networking strategy will be designed by taking into account:

- **Who:** to define the communities that can beneficiate of the projects outcomes
- **What:** to identify opportunities to start new collaboration among partners
- **How:** to identify a plan of activities and a list of opportunities to collaborate with other relevant projects (including the preparation of communication materials and tools)

These will be described in detail in the next sections.

Finally, an overall assessment of the community building activities will be performed in order to measure the activities impact. An internal evaluation will help to keep the desired level of networking and dissemination and allow us to correct any deviations from the goals of this WP. A set of **Key Performance Indicators (KPI)** will be used to monitor the progress in networking. They are reported in Table 1 and complement the set of KPIs defined in the description of the work.

Table 1: Networking KPIs

Networking tool	KPI	Objective	Contingency plan
Partners participation in previous Projects related to Cloud	Number of projects	10	The aim is to achieve a map of partner's projects and monitoring how their participation in EU proposals evolves during the project.
Usage of Social Networks[1]	Activity and Number of followers for each specific social tool	250	Experimentation of specific social network tool to identify the most suitable
Exchange programme for researchers training	Number of programmes	2 (for each Milestone)	Realise online courses to disseminate the project progress

[1] The Use of Social Network is a Key Performance Indicator directly connected with the performance indicators included in D6.4 (table 2)

3 Internal Networking strategy

MUSA Partners understand internal networking as the way to explore singular partner background, with the goal of identifying better ways to enlarge the network, encourage new collaborations among partners and individuals, identify stakeholders' interest in project results and to create new opportunities for spreading the project results.

The aim of this section is to define a strategy for building a strong network among MUSA members, trying to empower the dowry of experiences that each institution brings into the consortium as a whole.

We want to endorse the researchers as a main part of the network, listing people that are involved in the project and highlighting:

- Interest of research and skills,
- Previous projects carried out about Cloud and Security,
- Scientific background and publications.

The plan of internal networking activities includes:

Development of a catalogue of researchers

In order to collect specific skills and research interest, we will develop a catalogue of researchers that will be published on the MUSA web site for describing each participant's profile according to a simple template reported in Section 3.1.

Finding collaboration opportunities

Starting from the collaboration on specific tasks, we need to find a way to enlarge the project experience, finding new opportunities as:

- Participation in conferences (as described in the D6.2 *Dissemination Strategy*)
- Collaboration on specific tasks for the development of a new Cloud security framework
- Research papers

Promote trust and knowledge exchange

In order to encourage the trust and knowledge exchange, networking aims to spread the following activities:

- Researchers exchange,
- Conferences participation,
- Face to Face meetings,
- Preparation of new proposals,
- Students internship,
- Presentation of case studies with representatives from industrial sectors,
- Organisation of seminars.

In the following subsection the information pointed out through the catalogue of researchers is reported.

3.1 Description of MUSA partners

The catalogue of researchers is aimed at identifying each component of MUSA work team. For each researcher, we will create a profile on the MUSA Catalogue of researcher. This will be an online tool, designed to empower the wealth that is embedded in the experience of any person contributing to MUSA result. The catalogue of researchers proposes a tool that allows a better knowledge of the networking members and involved competences. At this level, the focus is on the human resources

that contribute with their intellectual activity to the project success and contribute to improve the knowledge of each researcher background.

Each researcher involved in the partner team has to fill in its profile. The description will contain short information about researcher profile as reported in the following table.

Table 2: MUSA team member information

Member	MUSA Partner Reference	Short CV			Information Shared for MUSA
		Skills	Main Publications	Related Publications	

The inputs gathered from MUSA members will be presented in the project web site, through the design of dedicated page. The information publicly available will be given using a graphic frame in line with MUSA communication tools.

4 External Networking strategy

The networking activities aim at exploiting synergies between the projects and increasing the impact of the ICT initiative. In particular, the activities here reported, aim at exploiting synergies between MUSA and other projects and will primary consist of contributions to working groups, participation in workshops and events, joint dissemination activities and production of joint dissemination materials. Nonetheless, given the features of the MUSA consortium, we will focus our attention on strategies to approach commercial developers, too.

This section describes the details on the external networking strategy in order to primary build up thematic clusters with other projects and research teams as well to target the commercial developers community for better exploit the MUSA results. This will be done not only through the dissemination activities described in deliverable D6.2 but also with dedicated channels and commercial strategies provided by MUSA partners.

4.1 MUSA partners of the external network (Who)

As described in the previous section, the first level of the MUSA network (internal) is made of all MUSA partners. In the networking building process, each MUSA partner will identify and possibly engage external "nodes" for synergies. In particular, the external nodes we want to target will include:

- Partners of other EU/National projects directly connected with MUSA partners and interested in the project results;
- ICT Society and/or associations,
- Different clusters of stakeholder identified for types of interests,
  - Public Institutions (EU /National),
  - Commercial,
  - Academic,
  - Research Centers

4.2 Networking Activities (What)

The activities presented in this deliverable, complement the dissemination activities described in deliverable D6.2, where dedicated channels have been identified (web tools, social networks, scientific papers, industrial presentations….). In particular, the networking plan will include:

- Identification of what is worth of being shared;
- Identification of networking opportunities and related channels.

The following sections present an initial analysis of these two crucial aspects. These lists will be periodically updated and integrated in order to take the best opportunities.

4.2.1 Identification of what is worth of being shared

In order to raise awareness and interest on the targeted audience during the networking activities it is important to highlight different aspects/features of the MUSA project. The main aspects that are worth of being shared are:

- Expected results,
- Innovative aspects,
- Real case studies,
- Benefits.

The MUSA partners involved in the networking activities should refer to this list as a reference motivating the networking activities. The list, detailed below, is aligned with the content of the description of work of the MUSA project.

Expected results:

- MUSA framework,
- MUSA Integrated Development Environment (IDE),
- MUSA security libraries:
  - Monitoring,
  - Enforcement,
  - Notification.
- MUSA decision support tool,
- MUSA distributed deployment tool,
- MUSA monitoring service,
- MUSA enforcement support service,
- MUSA notification service,
- MUSA security assurance platform (SaaS),
- Guide for an integrated multi-cloud secure applications lifecycle management.

Innovative aspects:

- Design and development of multi-cloud secure applications,
- Security-aware SLA,
- Composite multi-cloud application SLA,
- Security-driven decision support for cloud service selection and distributed deployment,
- Security assurance at runtime, including monitoring, enforcement and notification.

Real case studies:

- Airline flight scheduling by Lufthansa Systems,
- Smart mobility in Tampere City.

Benefits:

- Increase the quality of user experience and trust in clouds,
- Simplify the overall process of integrating security in clouds (DevOps),
- Promote the use of clouds in industry by boosting its security,
- Allow the incorporation of security requirements since the very beginning of the development process,
- Centralized control point to monitor security of multi-cloud applications.

4.2.2 Identification of external networking activities

The networking strategy includes a list of activities to ensure the effectiveness of networking, to engage all partners to have benefits according to their profile (academic or industrial) and, finally, to introduce some quality control and monitoring procedures through the adoption of Key Performance Indicators (KPI).

In particular, the activities here reported, aim at primarily exploiting synergies with other projects and will consist of organization and participation to workshops and events, collaboration with other EU projects and working groups, looking for joint dissemination activities. Nonetheless, given the features

of the MUSA consortium, we will focus our attention on strategies to approach commercial developers, too.

Dissemination and networking activities, including:

- Publication of research papers,
- Conferences organization and participation,
- Preparation of new proposals,
- Researchers exchanges,
- Seminars.

Organization of Community-building events, including:

- MUSA intermediate workshop: the main purpose of the workshop is to focus on a particular research theme. Date: M20 (September 2016)
- MUSA final workshop: the main purpose of the workshop is to present project results and to encourage focus on particular research themes to develop new ideas and proposals. Date: M30 (December 2016)

Finding networking opportunities, including:

The collaboration with other EU projects is one of the main networking opportunities; the MUSA partners are already members of other projects and they plan to promote active and proficient collaborations to create positive synergies on Cloud and Security related scientific results. Furthermore, this activity will give continuity to research and innovation in the context of other EU-funded projects of the FP7 and CIP Programmes and includes:

- **Collaboration with other EU funded projects**, as described in details in Section 4.3.1.
- **Participation in thematic clusters,** as described in details in Section 4.3.2.

Commercial networking activities:

Given the number of industrial partners in the MUSA consortium, we will dedicate activities on strategies to approach commercial developers, too. These will be described in detail in Section 4.3.3.

4.3 Networking Opportunities (How)

MUSA is open to collaborate with other EC funded projects and other initiatives on technical topics that are of joint interest. This means that MUSA will actively seek collaboration with other projects and initiatives in the areas of Data Protection, Security and Privacy in the Cloud.

To this end, all partners will contribute and especially the ones who actually carry out the technical work. The networking will not only be addressed at a management level but at a technical as well.

4.3.1 EU funded projects in the field of Cloud Computing and Internet Services

The following table presents those European projects related to MUSA and potential candidates to network its research and results.

Table 3: European projects potentially interested in MUSA results

Project	Objective	Web Site	EU Programme Call
CLARUS	It is focus on improving trust in cloud computing and securely unlocking sensitive data to enable new and better cloud services. CLARUS is developing a secure framework for storing and processing data	www.clarussecure.eu	H2020-ICT-2014-1

Project	Objective	Web Site	EU Programme Call
	outsourced to the cloud so end-users can monitor, audit and control their stored data while gaining the cost-saving benefits and capacity that cloud services bring		
ESCUDO-CLOUD	It aims at empowering data owners as first class citizens of the cloud. ESCUDO-CLOUD provides effective and deployable solutions allowing data owners to maintain the control over their data when relying on Cloud Service Providers (CSPs) for data storage, processing, and management, without sacrificing on functionality.	www.escudocloud.eu	H2020-ICT-2014-1
SERECA	It aims at removing technical impediments to secure cloud computing, and thereby encourage greater uptake of cost-effective and innovative cloud solutions in Europe. It proposes to develop secure enclaves, a new technique that exploits secure commodity CPU hardware for cloud deployments, empowering applications to ensure their own security without relying on public cloud operators.	www.serecaproject.eu	H2020-ICT-2014-1
SLALOM	It provides additional assurance for the uptake of cloud services with its SLA model legal clauses and technical specifications, using a trustworthy base, which is practical, fair, and understandable, while saving time and resources.	slalom-project.eu	H2020-ICT-2014-1
SLA-READY	It aims at giving pain relief to cloud customers through a service-driven approach specifically designed for SMEs. SLA-Ready will shed a new light on Cloud Computing through a service driven approach that will guide SMEs through their Cloud journey. The project will provide practical guides, user-friendly tutorial and decision making support tools will help SMEs understand what to expect and what to look out when signing up with a cloud provider in order to get the best deal.	www.sla-ready.eu	H2020-ICT-2014-1
SWITCH	It addresses the urgent industrial need for developing and executing time critical applications in Clouds. SWITCH addresses these problems by providing an interactive and flexible software workbench that can provide the necessary tools to control the lifecycle for rapid development, deployment, management and dynamic reconfiguration of complex distributed time-critical Cloud applications.	www.switchproject.eu	H2020-ICT-2014-1
SPECS	It aims at developing and implementing an open source framework to offer Security-as-a-Service, by relying on the notion of security parameters specified in Service Level Agreements (SLA), and also providing the techniques to systematically manage their life-cycle.	www.specs-project.eu/#	FP7-ICT-2013-10
A4CLOUD	It focuses on the Accountability For Cloud and Other Future Internet Services as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based	www.a4cloud.eu	FP7-ICT-2011-8

Project	Objective	Web Site	EU Programme Call
	IT services. The research being conducted in the project will increase trust in cloud computing by devising methods and tools, through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in the cloud.		
TRESCCA	It aims to lay the foundations of a secure and trustable cloud platform by ensuring strong logical and physical security on the edge devices, using both hardware security and virtualization techniques while considering the whole cloud architecture.	www.trescca.eu	FP7-ICT-2011-8
CLIPS	It brings together key stakeholders from across the EU including Public Authorities, Citizens and Businesses to develop a dedicated framework for cloud based public services which seeks to overcome some of the major issues that have so far prevented the full adoption of the cloud within the public sector notably in architecture, design and security.	www.clips-project.eu	CIP-ICT-PSP-2013-7
PAASWORD	It will introduce a holistic data privacy and security by design framework enhanced by sophisticated context-aware policy access models and robust policy access, decision, enforcement and governance mechanisms, which will enable the implementation of secure and transparent Cloud based applications and services that will maintain a fully distributed and totally encrypted data persistence layer, and, thus, will foster customers' data protection, integrity and confidentiality, even in the case wherein there is no control over the underlying third-party Cloud resources utilized.	sites.google.com/site/paaswordeu	FP7-ICT-2013-10
COCO CLOUD	It aims at allowing the cloud users to securely and privately share their data in the cloud. This will increase the trust of users in the cloud services and thus increase their widespread adoption with consequent benefits for the users and in general for digital economy.	www.coco-cloud.eu	FP7-ICT-2013-10
CloudWATCH	It aims at ensuring high visibility of European R&D cloud initiatives driving interoperable solutions & services. CloudWatch, in 24 months, will accelerate and increase the use of cloud computing across the public and private sectors in Europe and strengthen collaborative, international dialogue on interoperability and portability. Three Concertation Meetings will support organisations, fostering multi-stakeholder dialogue and cross-fertilisation on best practices. CloudWatchHUB.eu will raise awareness of the benefits to major stakeholder groups: enterprises, especially SMEs; governments and public authorities; research and education institutions. CloudWatch will make an active contribution to standards and certification, driving	www.cloudwatchhub.eu	FP7-ICT-2013-10

Project	Objective	Web Site	EU Programme Call
	interoperability as critical to broadening choice and boosting innovation. It will provide a portfolio of EU and international use cases that demonstrate interoperability, portability and reversibility. CloudWATCH ends on the 31th of August 2015, but it is expected that their cloud supporting activities will continue in the form of extension of the project named CloudWATCH2.		
PaaSage	PaaSage will deliver an open and integrated platform, to support both deployment and design of Cloud applications, together with an accompanying methodology that allows model-based development, configuration, optimisation, and deployment of existing and new applications independently of the existing underlying Cloud infrastructures. Specifically it will deliver a CLOUD modelling language, an IDE (Integrated development environment), execution-level mappers and interfaces and a metadata database. The Consortium bring together ERCIM for management and STFC as scientific coordinator together with experts in different aspects of CLOUDs ranging from software and services (SINTEF), High Performance Computing (HLRS) and systems development environments (INRIA) to a group of SMEs working on CLOUD systems and end-user organisations with requirements in the CLOUD domain.	www.paasage.eu	FP7-ICT-2011-8
MODAClouds	The main goal of MODAClouds is to provide methods, a decision support system, an open source IDE and run-time environment for the high-level design, early prototyping, semi-automatic code generation, and automatic deployment of applications on multi-Clouds with guaranteed QoS. Model-driven development combined with novel model-driven risk analysis and quality prediction will enable developers to specify Cloud-provider independent models enriched with quality parameters, implement these, perform quality prediction, monitor applications at run-time and optimize them based on the feedback, thus filling the gap between design and run-time. Additionally, MODAClouds provides techniques for data mapping and synchronization among multiple Clouds.	www.modaclouds.eu	FP7-ICT-2011-8

4.3.2 Clusters and Collaboration Working Groups

The main networking channel for MUSA project will be the Cluster on Data Protection, Security and Privacy in the Cloud (DPSP Cluster), initiated by the DG-CNECT E2 Unit of the European Commission.

This cluster was born with the aim to seek synergies between these projects and to join efforts towards greater impact.

The topics addressed in the cluster give continuity to research and innovation in the context of other EU-funded projects of the FP7 and CIP Programmes.

The project manager of MUSA is coordinating the cluster together with the support of Francisco Medeiros Deputy Head of Unit of DG-CNECT.

The main initial objectives of this cluster are:

1. Maximize the impact of EU-funded research and innovation project results in the areas of Data Protection, Security and Privacy in the Cloud by:
   - Seeking synergies in the methods, tools and solutions proposed by EU-funded research and innovation projects in the areas of Data Protection, Security and Privacy in the Cloud.
   - Maximizing the innovation over state-of-the-art and the advances on the common research areas.
   - Collaboration in the organisation of joint dissemination events, such as joint Workshops and conferences, and collaboration in other joint dissemination actions such as joint papers and articles, etc.
   - Joint efforts to encourage standardisation whenever possible.
2. Ensure the market orientation and adoption of EU-funded research and innovation project results in the areas of Data Protection, Security and Privacy in the Cloud by:
   - Working in the deep analysis of market trends and needs in the areas of Data Protection, Security and Privacy in the Cloud.
   - Looking for alignment of exploitation strategies and models of EU-funded research and innovation project results as much as possible.
3. Help to define the research and innovation needs in H2020 in the areas of Data Protection, Security and Privacy in the Cloud by:
   - Contributing to the definition of strategic research areas and topics for the strategic and work programmes.
   - Providing feedback on the drawbacks and problems faced during the execution of the projects with respect to the impact achievement in order to look for solutions in future projects.

The cluster aims to serve as an instrument to ease the achievement of market impact of the participating projects. Therefore, the main idea is that the participation in the cluster does not become an extra effort for the participating projects, but integrates with the projects' interests in creating greater impact. The cluster organizes periodic meetings by teleconference (every two months at least) and the first face-to-face meeting of the Cluster will be held on the 7th of October in Pisa, under the umbrella of the Cloud Forward First International Conference organized by the HOLA CLOUD EU project. In that meeting the cluster will set up the schedule of future cluster meetings and face-to-face meetings for continuous collaboration and experience sharing. At the time of writing, the Cluster is in the process of defining the specific joint results and joint dissemination events that it will deliver.

More information on the DPSP Cluster is available online in the Cluster Website: https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

The DPSP Cluster website has a Private area for the Cluster members to collaborate and share documents and results.

In addition, there are more opportunities to work together with other stakeholders of MUSA for facilitating the sharing of the results. In the following, we provide a list of the initially identified activities:

a) **Concertation of EU-funded research projects**: MUSA collaborates in the concertation activities organized by CloudWATCH too. This includes the participation in the Concertation email group and attending Concertation events: Concertation Meetings (every six months approx.). MUSA was presented for the first time at the Net Futures 2015 event (25 March 2015,

Brussels) were the Concertation meeting took place, and the MUSA presentation was included in the project portfolio distributed in the event. The Concertation Meeting looked at future directions for software services and cloud in Europe, highlighting new opportunities for novel research and innovation to ensure Europe remains a world leader (http://www.cloudwatchhub.eu/turning-cloud-research-innovative-software-services). MUSA project manager will attend relevant meetings organized by CloudWATCH, e.g. the Cloud Standards Profile Workshop - 24 Sept, Brussels.

b) **Participation in the ICT 2015 - Innovate, Connect, Transform, on 20-22 October 2015 in Lisbon, Portugal**. MUSA contributed to the proposal of a winning networking session together with other projects on the Cloud: *Privacy, Certification and SLA for dependable clouds*. (https://ec.europa.eu/digital-agenda/events/cf/ict2015/item-display.cfm?id=15464). The project with which MUSA will collaborate there are: CLARUS, SLA-Ready, CUMULUS, MUSA, SLALOM, and SPECS. MUSA will participate in that networking session contributing with the advances on security properties for multi-cloud applications.

c) **Participation in the Cybersecurity & Privacy Innovation Forum** (yearly). MUSA attended the CSP Innovation Forum 2015 (http://www.cspforum.eu/2015) on 28-29 April 2015, Brussels, and the MUSA project manager is member of the Programme Committee of the conference. The CSP Innovation Forum 2015 is supported by A4CLOUD, ATTPS, IPACSO, PRIPARE, SECCORD, SECURED, TREsPASS projects.

d) **Collaboration with HOLA CLOUD EU Project (http://www.holacloud.eu/).** The HOLA Cloud project is a CSA co-funded by the European Union that started on 1st January 2015 and will end on 31st December 2016. HOLA CLOUD targets to establish effective mechanisms for efficient collaboration among the members of the software, services and Cloud computing community. MUSA will participate in the Cloud Forward First International Conference organized by HOLA CLOUD, 6th of October, Pisa.

4.3.3 Strategy for commercial networking with MUSA stakeholders

MUSA is a project oriented to provide a framework for the development of secure multi-cloud applications. This solution will be interesting for all MUSA stakeholders identified in deliverable D1.1 *Initial MUSA framework specification*:

- End-user: the customer of multi-cloud applications developed with MUSA framework.
- System Operator: system managers that deploy applications in multi-cloud environments.
- Service Administrator: responsible for the management and monitoring of the multi-cloud applications at runtime.
- Service Business Manager: responsible for the business aspects of multi-cloud applications.
- Application Developer: developers of applications or services for multi-cloud environments.
- Application Architect: architects of multi-cloud applications or services.
- Security Architect: specialisation of Application Architect, in charge of ensuring secure design of multi-cloud applications.

In the following the industrial partners of MUSA provide the initial plans for commercial networking with such stakeholders.

Montimage strategy:

To be able to reach all these stakeholders, Montimage will participate in a series of public events, social networks campaign, and scientific publications with the aim of making the MUSA developments as much known as possible, including information in its website and the distribution of the MUSA flyers in those venues where it participates. Furthermore, the open-source developments within the MUSA framework will be publicly available in the GitHub platform, giving access to a large community of developers, looking for participants to develop both applications based on the MUSA framework and new modules to be part of it.

For each group of stakeholders, Montimage has planned a different strategy to approach them and to publicize the MUSA developments:

Table 4: Montimage strategy

Stakeholder	Strategy
Application developers	• Availability of open-source MUSA developments in GitHub, • Dissemination of public APIs and documentation to develop MUSA-compliant applications.
System Operators	• Participation in industrial venues to promote the MUSA developments.
System administrators	• Online availability of MUSA-related information and Social Networks campaign.
End users	• Advertising of the MUSA benefits in Social Networks and specialised websites.
All MUSA stakeholders	• Intense marketing campaign based on Social Networks and specialized websites, • Availability of MUSA-related information in Montimage's website, • Publication of MUSA results in specialised venues (both industrial and research-oriented), • Demonstration of the MUSA results in the IoT and Air transportation contexts.

AIMES strategy:

AIMES will primarily be engaging with other CSPs and Service Business Managers in regards to the MUSA Framework. The strategy to engage with these organisations consists of formal meetings, attendance of conference and demonstrations at relevant events.

The MUSA Framework will be exploited by 3 key divisions within the AIMES organisations

- R&D Development

  The MUSA Framework will be referenced and if at all possible expanded upon during future funded projects with the consortium and/or additional members

- Commercial

  Our commercial division will utilise the expertise gained during the project to promote the use of secure multi-cloud deployments to customers.

- Corporate Literature

MUSA will feature prominently within corporate literature to demonstrate the organisation's commitment to understanding the latest in cloud security

Currently our experience shows that Multi-cloud deployments are not being asked of AIMES. Often people want their infrastructure across different sites, but this isn't a true multi-cloud deployment. Communicating the MUSA framework to commercial entities will depend on the following criteria:

- BUDGET: Is there a budget for a multi-cloud deployment?
- AUTHORITY: Who has the authority to deploy a multi cloud application?
- NEED: Is there a need to deploy a multi-cloud environment?

  It would not make commercial sense to promote a multi-cloud deployment via the MUSA framework if there is no need.

- TIMEFRAME: Is there a timeframe for a multi-cloud deployment to be implemented?

That being said however, the MUSA Framework does consist of components that by themselves would be seen as an attractive proposition to AIMES current and prospective clients.

Table 5: AIMES strategy

Stakeholder	Strategy
System Operators	• Engagement with industry bodies such as Data Centre Alliance.
Service Business Managers	• Commercial engagements explaining the business benefits independently verified by the MUSA DST
End-users and Service Administrators	• Demonstration of the MUSA Framework including the benefits of Multi Cloud environments

LSY strategy:

LSY will primarily be engaging with the different entities in the group providing software solutions for the airline industry. This is done by using the existing collaboration tools, group-wide technology days, demonstration days within product lines, etc.

We identified the following groups of stakeholders and possible strategies to approach them:

Table 6: LSY strategy

Stakeholder	Strategy
Application architects and Security Architects	• Inform them about the MUSA framework and how to make use of the security-by-design principle to create MUSA compliant and secure applications, • Explain them the benefits of using MUSA.
Application Developers	• Make developer and DevOps teams aware of the APIs, the development tools and technologies related to MUSA (e.g. the MUSA IDE, the MUSA library etc.), • Inform about the possibilities during runtime.
End users and external partners	• Demonstration of the MUSA features to create secure applications running in the cloud. • This is done during workshops and industrial fairs like the annual LSY Airline Forum (e.g. https://youtu.be/Z-rabjQZfqk).

CA strategy:

CA is a worldwide organisation that has development teams in many locations. Our core strategy is the management and security of ICT. There are a number of groups that we interact with both in CA and externally. The different groups require different approaches:

CA technical staff including pre-sales and consulting:

There are several existing routes to disseminate information about MUSA.

1. There are regular "Tech Talks" for the whole of CA to listen to Webex presentations of interesting technologies. This is the widest audience within CA and the presentations are recorded. As the project progresses presentations based on milestones and significant discoveries will be delivered through "Tech Talks".
2. CA's Council for Technical Excellence has scheduled meetings where a MUSA presentation would reach across the development and sales organisation's top technicians. This group is also

responsible for the CA Technology Exchange online magazine (See below under external outreach).

3. CA strategic research is discussed regularly with CA product management teams to transfer knowledge that will influence the research but also with the potential to be included in the development backlog for inclusion in future products.

External Outreach:

In addition to CA technical staff, other stakeholders will be approached as indicated in next table.

Table 7: CA strategy

Stakeholder	Strategy
Application architects, Security Architects and Application Developers	• CA World is CA's worldwide sales and technology convention held approximately every 18 months. MUSA is not mature enough for presentation at the developer section of this convention in November 2015 but will be mature enough for consideration as a session in Spring 2017. • Software engineering development conferences. CA strategic research is engaged in writing and presenting papers to academic and trade conferences and these papers always generate interest and contacts/discussions.
All MUSA stakeholders	• Customer Outreach is a program that is being developed and enhanced within strategic research. This program enables CA staff engaged in MUSA to meet CA customers who have an interest in research and present the status and products of research products. MUSA is of interest because of the prominence of Cloud Computing security in the list of concerns expressed by analysts and customers. • CA Technology Exchange is an online magazine with a world wide circulation. There are quarterly topics chosen and articles are published on those topics on a rolling schedule. MUSA overview and Decision Support in choosing APIs have already been published.

References

[1] MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017. www.musa-project.eu

[2] "Towards Self-Protective Multi-Cloud Applications - MUSA – a Holistic Framework to Support the Security-Intelligent Lifecycle Management of Multi-Cloud Applications" In Proceedings of CLOSER 2015, Lisbon, 20 May 2015. http://closer.scitevents.org/

[3] Marsden P. (1981) "Introducing influence processes into a system of collective decisions", American Journal of Sociology , 86 pp.1203-1235

[4] Smart Specialisation Available at: ec.europa.eu/research/regions/index_en.cfm?pg=smart_specialisation. (Retrieved September 2015)

[5] Cohesion policy 2014-2020. Available at: ec.europa.eu/regional_policy/archive/what/future/index_en.cfm (Retrieved September 2015)

[6] European Commission. Digital Agenda for Europe. 2014. Available at: ec.europa.eu/digitalagenda/ (Retrieved April 2014)

[7] European Commission, "Progress on EU data protection reform now irreversible following European Parliament vote," vol. MEMO/14/186, March 2014. Available at: http://europa.eu/rapid/pressrelease_MEMO-14-186_en.htm (Retrieved April 2014)

[8] European Commission. "Proposed Directive on Network and Information Security – frequently asked questions". MEMO/13/71. 2013. Available at: http://europa.eu/rapid/press-release_MEMO-13-71_en.htm (Retrieved April 2014)

[9] European Commission. "Great news for cyber security in the EU: The EP successfully votes through the Network & Information Security (NIS) directive". STATEMENT/14/68. March 2014. Available at: http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm (Retrieved April 2014)

Appendix A. MUSA motivation and background

The main goal of MUSA is to support the security-intelligent lifecycle management of distributed applications over heterogeneous cloud resources, through a security framework that includes: a) security-by-design mechanisms to allow application self-protection at runtime, and b) methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications.

MUSA overall concept is depicted in the figure below.

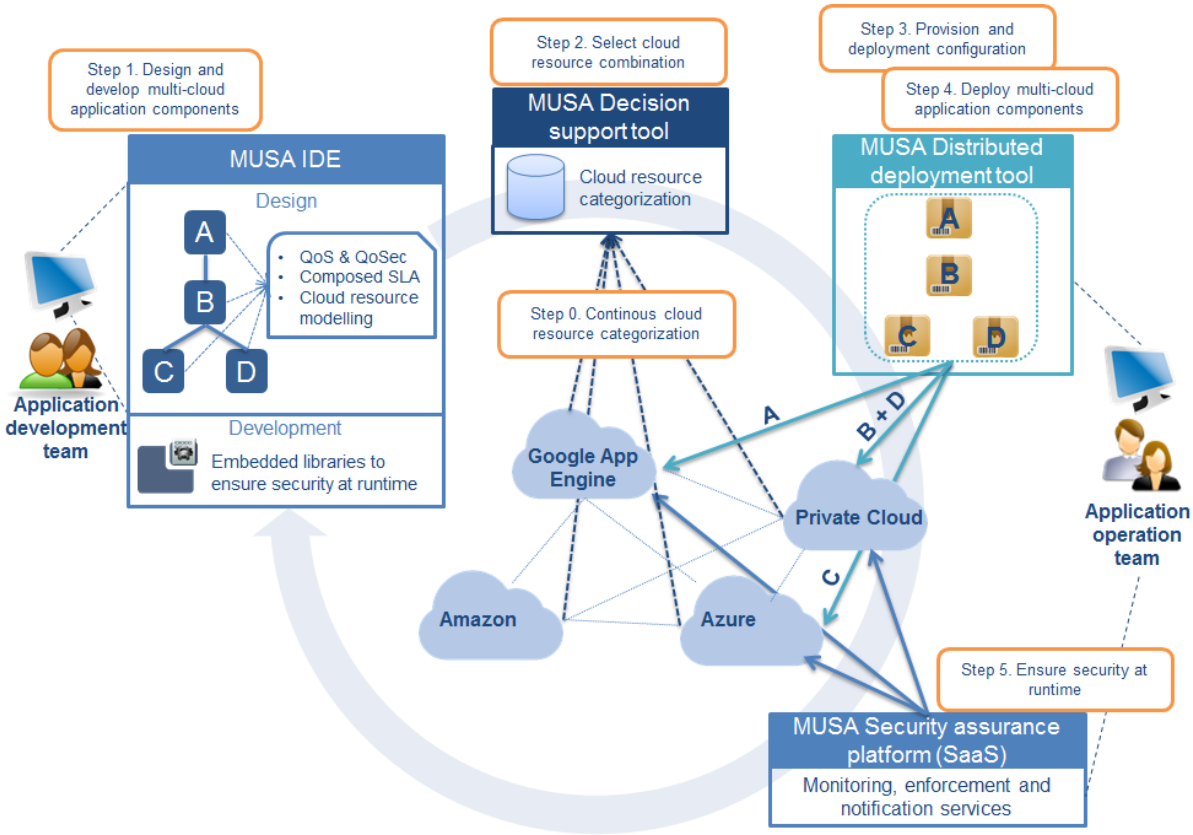

Figure A.1: MUSA overall concept

MUSA framework combines 1) a preventive security approach, promoting Security by Design practices in the development and embedding security mechanisms in the application, and 2) a reactive security approach, monitoring application runtime to mitigate security incidents, so multi-cloud application providers can be informed and react to them without losing end-user trust in the multi-cloud application. An integrated coordination of all phases in the application lifecycle management is needed in order to ensure the preventive oriented security to be embedded and aligned with reactive security measures.