NEWSLETTER

March 2017

MULTI-CLOUD SECURE APPLICATIONS

WELCOME!!!

SECOND EDITION OF MUSA NEWSLETTER

Hello!

It's been a bit over two years of the MUSA project and several developments have taken place since the first publication of the MUSA newsletter.

MUSA, an EU H2020 research and innovation project continues to focus on the development of tools for facilitating the integration of security in multi-cloud applications.

In this issue, we present the MUSA tools which collectively make up the MUSA framework. Other highlights are the MUSA benefits, MUSA project's first review, case studies development and evaluation, events, publications and project collaborations.

We hope you enjoy this newsletter and find it very informative.

Project Details:

Duration

January 2015 – December 2017

Total Budget

€ 3.5M

EU Programme

ICT-07-2014 - Advanced Cloud Infrastructures and Services. No. 644429. RIA - Research and Innovation action.

Participating Countries

Finland, France, Germany, Italy, Spain and United Kingdom.

Highlights:

MUSA Benefits: How MUSA can help you ensure security in Multi-cloud

MUSA framework offers an integrated tool suit for DevOps and Agile engineering of (multi-)cloud based applications addressing security in all the phases: design, deployment and operation. The framework supports risk analysis and selection of secure cloud services, and it is able to automatically deploy and monitor the distributed components and create the application Service Level Agreement. Different roles within DevOps teams will benefit from the use of the framework tools:

- Application developers will be able to better specify the deployment needs and the security Service Level Agreement (SLA), as well as embed in the application components the necessary mechanisms to monitor and enforce the security at runtime.
- System operators will be able to get most out of cloud by selecting the best cloud service combinations according to their security features and by automatically deploying the application components on top of the selected services.
- Service administrators can assure the secure behaviour of multi-cloud applications in operation, and minimize the security risks while keeping the users informed.
- Business managers will have a means for a better informed decision making when selecting cloud services.

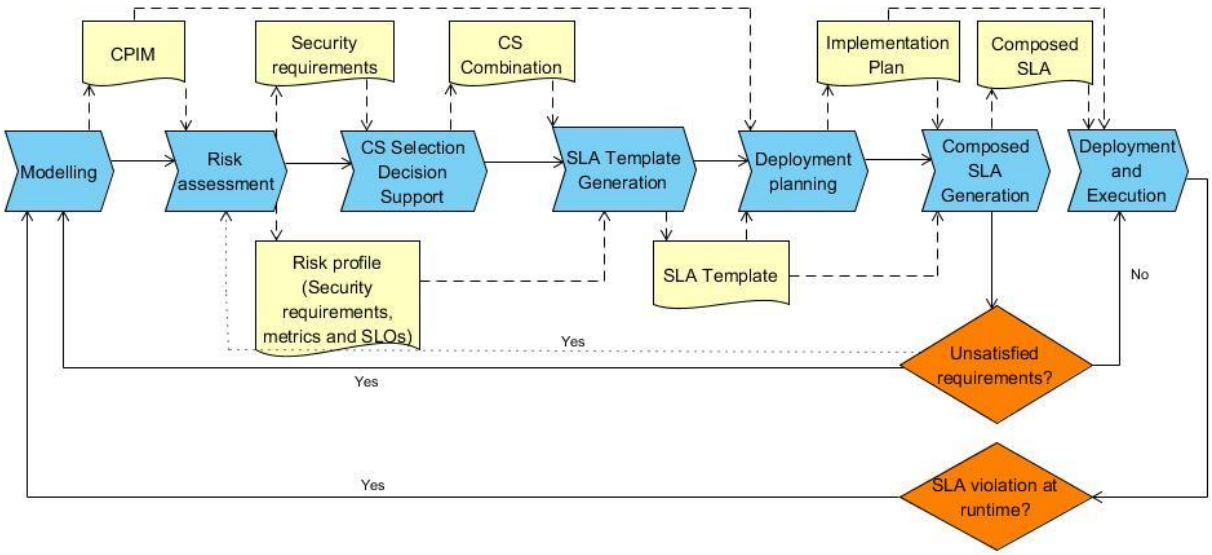
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644429

In summary, the data security incidents in multi-cloud applications will be reduced through the continuous assurance of a secure behaviour of individual cloud-based components and the overall application, even if the data are processed and/or stored by untrustworthy or opaque cloud providers.

The cloud consumers' trust on clouds will be enhanced by providing them tools for expressing their security needs and keeping them informed on the security and performance faults of the multiple cloud services in use.

MUSA FRAMEWORK

The MUSA Framework supports the security lifecycle management of a multi-cloud application.



During the **design phase**, the DevOps team first models the Cloud Provider Independent Model (CPIM) of the multi-cloud application using the MUSA Modeller. Then the DevOps team obtains the security requirements through the risk assessment process. Afterwards, together with the security requirements, the DevOps team can include other criteria such as business criteria and can search the best cloud services that match those criteria relying on the MUSA DST. Having selected the list of the cloud services that best match the requirements of the multi-cloud application and having previously defined the security requirements, the DevOps team can generate the SLA templates for the components of the multi-cloud application. These SLA templates will be stored in the SLA Repository and will be retrieved by the MUSA Deployer, so it can generate the implementation plan for the multi-cloud application. Once the implementation plan is generated, the MUSA Deployer shares it with the SLA Generator, so it can generate the composed SLA for the whole multi-cloud application.

Afterwards, at **deployment phase**, the MUSA Deployer is invoked by the DevOps team in order to deploy the multi-cloud application (by following the Implementation plan).

Finally, at **runtime** or **operation phase**, the MUSA Security Assurance Platform starts monitoring the multi-cloud application based on the final SLAs and the implementation plan. If the MUSA Security Assurance Platform detects any violation of the SLAs in place, it notifies the DevOps team and the multi-cloud application should be re-designed or re-deployed.

The main tools responsible for these activities are described next.

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

MUSA Dashboard

The MUSA Dashboard is a Kanban-style front-end web application, which allows the DevOps team to manage the design, deployment and operation lifecycle of a multi-cloud application on components basis. It enables DevOps to easily identify and understand the MUSA workflow and interact with the desired MUSA tool for each step.

The MUSA Dashboard video is available here.

MUSA Modeller

The MUSA Modeller is a web editor that allows the DevOps team to create and update the Cloud Provider Independent Model (CPIM) of a multi-cloud application in CAMEL format. Through these models it is possible to specify a complete specification of the requirements needed by an application to be deployed in a secure multi-cloud environment. The MUSA Modeller also allows the DevOps team to include MUSA security enforcement agents from the MUSA security catalogue in order to be automatically deployed by MUSA when the whole multi-cloud application is being deployed.

The MUSA Modeller video is available here.

MUSA Decision Support Tool

MUSA Decision Support Tool aims to ease up the tedious task of choosing the best cloud providers for the multi-cloud application to be deployed. Not only it considers the technical aspects of each of the application components, but it also ensures that the set of cloud providers chosen is the best possible from the non-technical perspective. The tool analyses the model of the application as well as the risk matrix to ensure the cloud service providers proposed are optimal for the given personalised deployment.

The MUSA Decision Support Tool video is available here.

MUSA SLA Generator

The SLA Generator allows to obtain a Security SLA of a (multi-)cloud application, allowing to define their security requirements from the very early stages of their development. The tool entails the adoption of risk analysis techniques, security assessment and SLA composition techniques aimed at identifying the main vulnerabilities affecting a cloud application and allows to determine the countermeasures to take into account at the design stage in order to thwart the main existing threats and assess the effective security. In particular, countermeasures are defined in terms of the security controls to apply (based on state-of-art Security Control Frameworks) and can be put in place by implementing specific security mechanisms to be integrated into the cloud application under development.

The MUSA SLA Generator video is available here.

MUSA Deployer

The MUSA Deployer allows the DevOps team to build an implementation plan and automatically execute the deployment (and re-deployment) of the components of a multi-cloud application. In order to execute the deployment, the MUSA Deployer acquires and configures the cloud services specified in the implementation plan, the deployment execution relies on Chef technology. The MUSA Deployer also copes with the security of the multi-cloud application by

(i) Acquiring the resources on selected CSPs that cover the security requirements by the DevOps team, and
(ii) Automatically deploying the security enforcement agents selected by the DevOps team with the functional application components. This aspect is one of the main innovative aspects of the proposed deployer.

The MUSA Deployer video is available here.

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

MUSA Enforcement Agents

The enforcement services to be offered in MUSA Framework are devised as mechanisms that could be easily integrated in multi-cloud application components and activated at runtime whenever needed. These security enforcement services are known as MUSA enforcement agents in the MUSA Framework and accessible to the MUSA Security Agents Catalogue. This catalogue is used by several MUSA tools such as MUSA Modeller and MUSA Deployer in order to include security features into the multi-cloud application deployment specification and automatically deploy them as part of the whole multi-cloud application.

MUSA Security Assurance Platform

The MUSA SAP (Security Assurance Platform) integrates mechanisms for runtime monitoring, security enforcement and alert notification. It is deployed as a service, and allows monitoring multi-cloud applications already deployed in different CSPs, performing the detection of potential deviations from the security SLAs, and automatically triggering countermeasures to enforce security during application runtime. It requires 4 main components to perform its operation:

- The security SLA repository, containing the security rules to be applied
- The MUSA Deployer, to recuperate the information regarding the deployed monitoring agents
- The monitoring agents, that are in charge of measuring the security metrics related to the required security controls
- The enforcement agents, which activate specific actions in case of security issues detection, with the ultimate objective of maintaining the confidentiality and privacy of sensitive data and communications.

The MUSA Security Assurance Platform video is available here.

MUSA Project 1st Review

The 1st review of the MUSA project was held on 5th October, 2016 in the premises of the European Commission in Brussels. According to the reviewers' opinion, the project had successfully met the objectives for the period and delivered good software pieces and deliverables, through an effective project management. The reviewers appreciated a lot the demonstrations made and noticed the high number of tools that the MUSA framework is integrating, providing support to the whole life-cycle of multi-cloud applications, from design to operation through deployment.

Due to the tool richness and complexity, the reviewers provided relevant feedback on how to better analyse and define the exploitation strategy, which needs to be carefully tailored to target customers that may differ from tool to tool in the framework. The partners committed to address the reviewers comments and suggestions in this direction.

As a general conclusion, the MUSA project was charged to continue with minor modifications.

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

PUBLICATIONS

The number of publications from MUSA project increased in 2016 as 8 papers were published as well as journals and articles in Technical magazines. They are listed below:

Conference Papers

- **Methodology to obtain security controls in multi-cloud applications**
  CLOSER 2016, Rome. (Partners: TUT, CERICT & Tecnalia)

- **SLA-driven monitoring of multi-cloud application components using the MUSA framework**
  STAM 2016, Nara, Japan. (Partners: CERICT, Tecnalia & Montimage)

- **Per-service security SLA: a new model for security management in clouds**
  WETICE 2016, Paris. (Partner: CERICT)

- **A Security SLA-driven methodology to set-up security capabilities on top of cloud services**
  SWISM 2016, Japan. (Partner: CERICT)

- **Scoring cloud services through digital ecosystem community analysis**
  EC-Web 2016, Porto. (Partner: CA)

- **Security: from Per-provider to Per-service security SLAs**
  SecureSysComm 2016, Ostrava, Czech. (Partner: CERICT)

- **Inter-cloud challenges towards free flow of data (Position paper)**
  CloudForward 2016, Madrid. (Partners: Tecnalia & CERICT)

- **Security-by-design in clouds: A Security-SLA driven methodology to build secure cloud applications**
  CloudForward 2016, Madrid. (Partners: Tecnalia & CERICT)

Journals

- **Enhancing security in cloud-based cyber-physical systems**
  Journal of Computing Research (JCCR), Published: October 2016.
  Partner: TUT

Technical Magazines

- **Multi-cloud computing: Select the right cloud services for a more agile development process**
  Cloud Strategy Magazine, Published: August 2016.
  Partners: CA, AIMES, LHS

- **Managing security in distributed computing: Self protective multi-cloud applications**
  ERCIM News, Published: October 2016.
  Partners: Tecnalia, CERICT & TUT

- **Cloud Computing** (*Available in Hungarian*)
  Innoteka Magazine, Published: November 2016.
  Partner: LHS

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

COLLABORATIONS

To enhance networking and collaboration with external organizations, other FP7 and H2020 related project as a means of seeking greater impact for project results and fostering synergies, MUSA was involved in the following collaboration activities;

- **Coordination of the DPSP Cluster**

MUSA currently serves as the coordinator of the DPSP cluster which involves 25 EU funded cloud research projects. The goal is to interact, find synergies and join forces to increase project impact. MUSA also successfully co-organized the first joint workshop of the cluster in February 2016 in Naples.

- **Collaboration with NATRES Cluster**

MUSA is a project member of NATRES which has about 20 project members. The aim of the cluster is to discuss current research and innovation challenges encountered at Infrastructure-as-a-service (IaaS) level.

- **Collaboration with Cloud projects**

MUSA has also been involved in collaborations with some of the cloud projects such as SPECS and PAASAGE for example. Areas of common interest were identified and has helped MUSA project to identify ways in which the MUSA results could be improved with existing works of the clustered projects.

- **Collaboration with CloudWATCH 2 project**

MUSA project continues to work closely with CloudWATCH 2 in order to identify best practices for overcoming challenges of standardization, interoperability and transparency of cloud services.

- **Collaboration with external organizations**

As a way of enhancing MUSA exploitation of MUSA key results, MUSA organized a workshop in conjunction with DCA, CSA and CIF in March 2016 in London. The discussion centered on CSP benchmarking. The outcome of the workshop led to further collaboration with other EU research projects; SLALOM and SLA-READY.

USE CASES

Two use cases are being carried out in the MUSA project as a way of validating the MUSA framework. Initial evaluation have been carried out in both use cases with the evaluators comprising a team of DevOps selected by the use case providers. Relevant feedbacks were also given. The main details are provided below:

Case Study A: Airline Flight Scheduling Multi-cloud Application

The Lufthansa System use case is a prototype of a web based flight scheduling application. The targeted flight scheduling application will consist of multiple independent micro service modules like: airport module, fleet module, airline module, schedule module, etc. All modules were designed following the DDD principles and applying the CQRS pattern. To avoid complexity in the prototype, we are concentrating only on a single module, the fleet module. To enable the fleet module further components are required: database, API gateway, security, message broker, webserver.

The security needs of the prototype are based on the application characteristic: the different modules provide interfaces to the single page web UI. The authentication and authorization of the users must be supported and handled in the backend. The high amount of components even deployed into different clouds needs to have a dashboard providing overview of the system with the ability to dig down into the details of a single component as well. The evaluators of the MUSA framework very much appreciated this kind of dashboard that supports the team work from the characterization of the application down to the runtime monitoring. In the first version of the MUSA framework they identified room for improvement for example on screens understandability and workflow support. Beyond these first weaknesses, the very promising MUSA concept was highly appreciated by the evaluators which included architect, developer, system administrator and even business decision maker.

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

Case Study B: Smart Mobility Multi-cloud Application

The Tampere use case is a smart mobility multi-cloud application. The application ensures secure, energy efficient, optimal and sustainable multi-modal urban travel experience for Tampere inhabitants. The application utilizes open data and it is composed of several components such as database, identity and access manager, consumption estimation calculator etc., which have been deployed in separate clouds in order to maintain a multi-cloud architecture. The use case involves the use of the personal data of users and as such, the main security needs addressed are privacy and data protection. In addition, the distributed nature of the application necessitated the provision of security across all components at the level of access and data transmission using secure channels and effective authentication, authorization mechanisms. Worthy of mention is the integration of the High Availability (HA) framework in the application to enforce relevant security requirements and controls.

Using the MUSA framework in the initial evaluation of the use case, the evaluators deployed and monitored the application components. In general, the MUSA framework was found to be effective in facilitating the required application security needs. However, some shortcomings were also identified and highlighted. Similarly to the other case study, the evaluators provided useful feedbacks on improving the overall efficiency, usability, interoperability and flexibility of the MUSA framework, and the project is committed to improve the solution by the end of 2017.

UPCOMING EVENTS

MUSA at Cloud Security Expo 2017

15–16 March 2017 Excel, London

http://www.cloudexpoeurope.com/

MUSA will actively participate at Cloud Expo Europe 2017, the biggest Cloud event in Europe. Last year the event gathered 515 technology buyers and influencers and this year, alongside Smart IoT, Cloud Security, Data Centre World and Big Data World, the show hosts 500 leading international technology exhibitor and 600 speakers.

The stand No. 1239:
MUSA will organise the **stand of the Data Protection, Security and Privacy in Cloud (DPSP) Cluster** of EU-funded projects. At the stand, the security and privacy innovations of 8 EU-funded research projects that participate in the DPSP Cluster will be presented to the visitors: MUSA, CLARUS, CREDENTIAL, CLOUDWATCH 2, OPERANDO, PAASWORD, PRISMACLOUD and SWITCH.

Besides the demos and presentations in the stand, on the **15th of March** the DPSP Cluster is also participating at:
• **Workshop** sessions that Cloud Watch 2 is kindly supporting, including:

- DPSP Cluster in 2017. - Chaired by MUSA coordinator. (9:00 - 9:50)
- Selecting and Switching Cloud Service Providers: The Challenges. - Chaired by CA Technologies partner. (10:30 - 11:50)
- Essentials towards a secure cloud for the Digital Single Market and future cloud market. - The MUSA coordinator will be one of the panellists. (14:00 – 14:50)
- GDPR Clinic - European General Data Protection Regulation: a Strategic Compliance Approach. (16:00 – 16:50)

• **Talks** by participants in the Cluster within the official programme., including these two of MUSA at the "Compliance and Governance & Cloud Security Strategies Theatre":

- The DPSP Cluster – Erkuden Rios (12:45 - 13:10)
- Controlling Risks by monitoring Cloud SLAs - Massimiliano Rak on MUSA innovations on Risk Analysis and security Service Level Agreement generation for (multi-)cloud-based applications. (15:15 - 15:40)

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

MUSA co-organises the SECPID Workshop at ARES Conference 2017

August 29 – September 1, 2017, Regio Calabria, Italy.

Under the umbrella of the Data Protection, Security and Privacy (DPSP) Cluster that MUSA coordinates, the project is co-organising the 2nd Workshop on Security, Privacy, and Identity Management in the Cloud.

The aim of this symposium is to provide a platform to discuss innovative ideas related to the following questions: How can cloud services be made more trustworthy? How can we build distributed systems without single point of failure or trust? How to design end-to-end secure services in an untrusted environment? Which methodologies and technologies are required to integrate security and privacy by design? Is it possible to give back users full control over which data they want to reveal, when and to whom?

Paper submission Deadline: April 15, 2017

MUSA co-organises the STAM Workshop at ARES Conference 2017

August 29 – September 1, 2017, Regio Calabria, Italy.

https://www.ares-conference.eu/workshops/stam-2017/

Just as last year, MUSA project is organising together with 4 other research projects the 2nd edition of the International Workshop on Security Testing And Monitoring.

The workshop is devoted to study how vulnerability, intrusions and attacks modelling can help users understand the occurrence of malicious behaviours in order to avoid them, and what are the advantages and drawbacks of the existing models. At the same time, the workshop tries to understand how to solve the challenging security testing and monitoring problem given that testing distributed systems is a complex task and security will add new challenges and difficulties to be solved.

The objective of this workshop is to share ideas, methods, techniques, and tools about security testing and monitoring in distributed systems to improve the state of the art. In addition to scientific paper presentations, we intend to have one or two keynotes describing ongoing activities in the related areas and demonstrations of some innovative security tools.

Paper submission Deadline: April 2, 2017

MUSA co-organises the TAROT Summer School 2017

June 26 - 30, 2017, Naples, Italy.

http://tarot2017.dieti.unina.it/

This year the project is organising the 13th TAROT Summer School on Software Testing, Verification & Validation. TAROT (Training And Research On Testing) is a network created to foster the mobility of students, faculty members and research scientists working in the field of testing and monitoring of software and communication systems. This summer school brings together lecturers, researchers, students and people from industry for one week of presentations, discussions and an opportunity to get to know each other. The TAROT Summer School is open to researchers working in the area of testing and monitoring, both from academia and industry.

Early registration closes: May 1, 2017. Do not miss it!

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

PAST EVENT

MUSA at Mobile World Congress 2017

27 February – 2 March 2017, Barcelona, Spain

https://www.mobileworldcongress.com/

As part of the Brokerage event, MUSA partner CA Technologies met with a number of potential customers at Mobile World Congress where they discussed the perceived benefits and drawbacks of multi-cloud approach and security challenges in multi-cloud environments. The feedback from the event was very valuable for the definition of the exploitation strategy in MUSA to better approach the market.

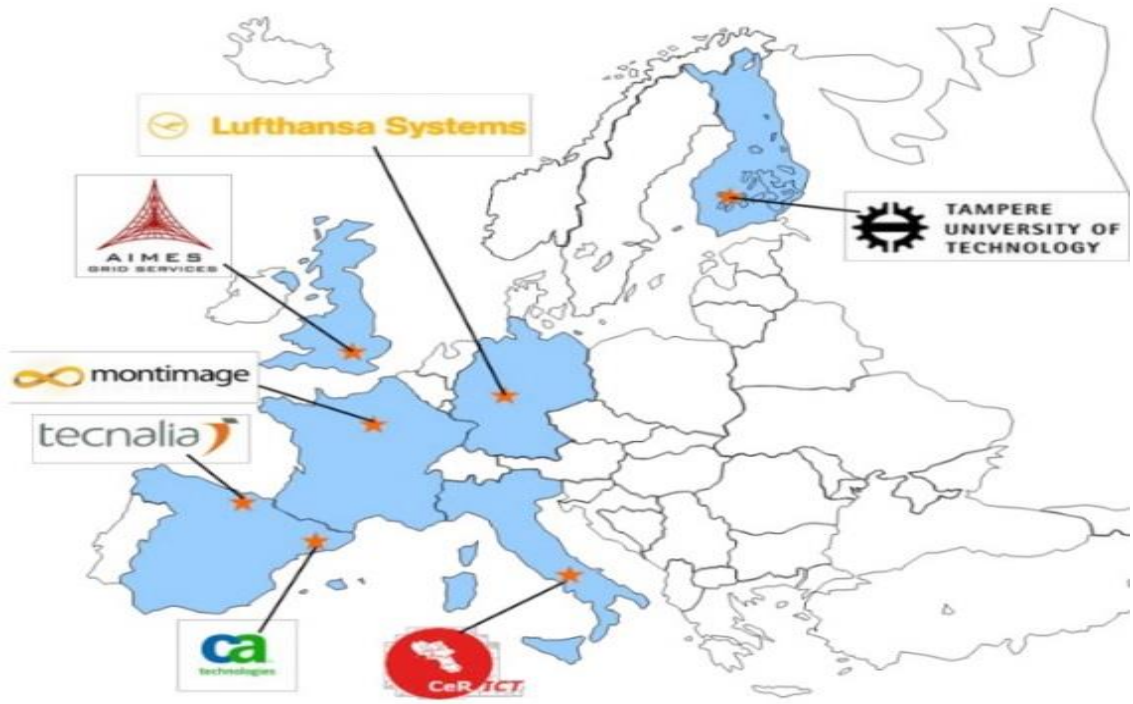
CONSORTIUM & CONTACTS

The MUSA project is coordinated by TECNALIA Research & Innovation who are based in Spain.

Project Coordinator
Erkuden Rios
erkuden.rios@tecnalia.com

MUSA website
www.musa-project.eu

@MUSA_project (https://twitter.com/MUSA_project)
MusaProjectEU (https://www.facebook.com/MUSAProjectEU)



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