**Project Details:**

**Duration**
January 2015 – December 2017

**Total Budget**
€ 3.5M

**EU Programme**

**Participating Countries**
Finland, France, Germany, Italy, Spain and United Kingdom.

**Highlights:**

MUSA Benefits 1-2
WHAT'S NEW 2-6
MUSA Evaluation 6
Final Review 6
Publications 7-8
Collaborations 6
Use Cases 6-7
Upcoming events 10-11
Consortium & Contacts 12

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

In agile collaboration between the developers of the tool and the Use Case the tool has been finalized.

The MUSA project is nearing its conclusion, and several developments have taken place since the publication of the last MUSA newsletter.

In this issue, we present the final changes to the tools, which collectively make up the MUSA framework. Other highlights are the MUSA benefits, MUSA project’s final review, events, publications and project collaborations.

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

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

MUSA framework offers an integrated tool suite 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.
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.

---

**FINAL MUSA FRAMEWORK**

The MUSA Framework is the first fully integrated and open source Security DevOps solution for multi-cloud applications. The Framework targets DevOps teams that deal with the security requirements and assurance of multi-cloud applications and supports their workflow with security-intelligent tools. The workflow can be seen in the picture below.

The workflow supported by MUSA Framework involves all the security activities required in the whole life-cycle of a multi-cloud application, from design to deployment and execution, i.e. operation.

Since the previous newsletter, the separate tools have been fully integrated into a single framework. The Framework offers an easy-to-use Dashboard in form of a Kanban-style board, for multi-disciplinary approach to security management. The MUSA Dashboard offers a role-based access control to the tools integrating the framework. The functionality and user interfaces of the tools have been revamped since initial versions for a more complete and professional user experience.

In the following sections, the final tools integrated in the framework are described.
MUSA Dashboard

The MUSA Dashboard is a Kanban-style front-end web application that is composed of six columns that represent different states in which the components of a multi-cloud application can be. It allows the DevOps team to manage the design, deployment and operation lifecycle of a multi-cloud application on component basis. It enables DevOps team to easily understand the MUSA workflow and interact with the required MUSA tool for each step.

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 MUSA-extended CAMEL format. The model captures the complete specification of the application requirements 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 Agents Catalogue so as they can be automatically deployed by MUSA when the whole multi-cloud application is being deployed.

MUSA Risk Analysis

The MUSA risk analysis allows DevOps team to use STRIDE methodology and identify the threats related to each component as well as assess the risk. Based upon the selected threats, it suggests a set of security controls needed to mitigate the threats. It mostly suggests security controls based on industrial standards defined by National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA).

MUSA Cloud Service Selection

The MUSA Decision Support Tool allows the DevOps team to review a list of cloud service combinations that best match the requirements of a multi-cloud application. It informs on the match-making percentage, so as the DevOps team can better decide on which deployment option selects, so the components of the multi-cloud application can be deployed there.

MUSA SLA Generator

The SLA Generator automatically generates the Security SLA of a (multi-)cloud application, allowing to define their security requirements from the very early stages of its development. The tool entails the identification of the desired security metrics over the security controls specified in the risk assessment process, as well as the computation of the composite Security SLAs of the application components taking into account the application architecture, deployment structure, nature of the components and Security SLAs of the cloud services used. The Security SLA composition is one the main innovations offered by the tool and consists in the computation of the security levels that can be effectively granted by the application.
MUSA Plan Deployment

The MUSA Plan Deployment allows the DevOps team to generate or retrieve a Implementation Plan associated with a multi-cloud application. The implementation plan can be reviewed and updated before moving on to the plan execution phase.

MUSA Deployer

The MUSA Deployer allows the DevOps team automatically executing the deployment (and re-deployment) of the components of a multi-cloud application. The deployment execution relies on Chef technology. The MUSA Deployer copes with the security of the multi-cloud application by:

(i) Acquiring and configuring the resources on selected CSPs from Cloud Service Selection step, and
(ii) Automatically deploying with the functional application components the security enforcement agents selected by the DevOps team. This aspect is one of the main innovative aspects of the Deployer.

MUSA Security Assurance Platform

The MUSA SecAP (Security Assurance Platform) 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. The platform integrates mechanisms for runtime monitoring and notification, security enforcement and reaction:

a) Monitoring Dashboard

The Monitoring Dashboard allows the System Administrator in the DevOps Team measuring the security metrics specified in the application components’ Security SLAs and visualising the status of the metrics. The monitoring informs on detected Security SLA violations and alerts (potential violations).

b) MUSA Reaction Dashboard

The Reaction Dashboard allows the System Administrator in the DevOps Team to configure reactions that are triggered by the application operator when an SLA alert or violation is detected by the monitoring part of the MUSA security assurance platform.

c) MUSA Enforcement Dashboard

The Enforcement Dashboard allows the System Administrator in the DevOps Team to configure and enable the deployed MUSA enforcement agents. Once enabled, it provides agent information such as events, states, etc. The available MUSA preventive enforcement agents include MUSA Identity Manager (IdM) and Access Control (AC) agents. In the future more agents are planned to be added.
MUSA Framework Evaluation

The evaluation in MUSA was a very dynamic process in the project lifetime. During the last months of the project it was intensified and the Tool developer partners and the Use case partners had a constant exchange of feedback about the tools. Technical and integration issues were fixed during this exercise. As a result, the framework was successfully finalized and the MUSA workflow was completed by the MUSA evaluators using the tools in the framework.

The feedback of the evaluators was encapsulated by a complete survey that each of them filled. As illustrated by the survey results, most the evaluators believe the tools to be very practical and innovative. In efficiency terms, the tools were evaluated very positively and, for usability, all the tools were accepted satisfactorily, though some of them received improvement suggestions to their graphical user interface. In general, the MUSA concept was highly appreciated and evaluators think that MUSA tools provide better services than the tools they currently use.

USE CASES

Two use cases have been carried out in the MUSA project as a way of validating the MUSA framework. Two formal evaluation rounds had been carried out in both use cases with the evaluators comprising a team of DevOps selected by the Use case provider partners. Relevant feedbacks were also given. The final evaluation took place on November-December 2017 after all the MUSA tools were integrated into a single framework. During the final evaluation, each Use Case partners utilized Final MUSA framework to create and completely deploy their application into production. 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 prototype consists 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, the evaluation concentrated only on some modules, like 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 very much appreciated this kind of dashboard that supports the team work from the characterization of the application down to the runtime monitoring. The very promising MUSA concept was highly appreciated by the evaluators which included architect, developer, system administrator and even business decision maker.

**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, multimodal journey planner, 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.

Using the MUSA framework in the Final evaluation of the use case, the evaluators modelled, deployed and monitored the application components. This use case fully integrated MUSA Access Control agent with their application and employed it to enforce secured access control of different types of users into their application. The systematic risk analysis and the automatic generation of the security SLA together with MUSA SecCAP were highly appreciated.

More information about the deployed application can be found in the link below:

http://tsm.musa-project.eu

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 644429
The number of publications from MUSA project increased in 2017 as 20 papers were published as well as journals and articles in Technical magazines. They are listed below:

**Conference Papers**

- An Automatic Tool for Benchmark Testing of Cloud Applications  
  7th International Conference on Cloud Computing and Services Science, Porto, Portugal (Partner: CERICT)

- Secure microGRID in cloud: The CoSSMic Case Study  
  GPC 2017, Cetara, Italy (Partner: CERICT)

- Security Assurance of (Multi-)Cloud Application with Security SLA Composition  
  GPC 2017, Cetara, Italy (Partner: CERICT)

- Towards Model-Based Security Assessment of Cloud Applications  
  GPC 2017, Cetara, Italy (Partner: CERICT)

- Multi-cloud Applications Security Monitoring  
  GPC 2017, Cetara, Italy (Partners: MI, Tecnalia)

- Security-Centric Evaluation Framework for IT Services  
  GPC 2017, Cetara, Italy (Partners: CA, Tecnalia)

- A platform for security monitoring of multi-cloud applications  
  The A.P. Ershov Informatics Conference, Moscow, Russia (Partner: MI)

- MUSA Deployer: Deployment of Multi-cloud Applications  
  WETICE 2017, Poznan, Poland (Partners: CERICT, Tecnalia)

- Providing an access control layer to web-based applications for the industrial domain  
  INDIN 2017, Emden, Germany (Partner: TUT)

- A Security Metric Catalogue for Cloud Applications  
  SWISM 2017, Torino, Italy (Partner: CERICT)

- Self-healing Multi-cloud Application Modelling  
  SECPID Workshop, 2017

- SLA-based continuous security assurance in multi-cloud DevOps  
  ESORICS 2017, Oslo, Norway (Partners: TECNALIA, ERICT, MI)

- Processing mobility traces for activity recognition in smart cities  
  SOCNE 2017, Beijing, China (Partner: TUT)

- Principles and risk assessment of managing distributed ontologies hosted by embedded devices for controlling industrial systems  
  IECON 2017, Beijing, China (Partner: TUT)

- Dynamic security assurance in multi-cloud DevOps  
  CNS 2017, Las Vegas, USA (Partners: Tecnalia, CERICT, MI)
• Agile Risk Management for Non-functional Requirements in Software Development
  REFSQ18, Utrecht, The Netherlands (Partner: CA)

**Journals**

• Per-service Security SLAs for Cloud Security Management: Model and Implementation
  International Journal of Grid and Utility Computing (Partner: CERICT)

• Airline Application Security in the Digital Economy
  Digitalization Cases Springer book (Partners: LHS, CA, Tecnalia)

• Security-by-design in Multi-Cloud Applications: an Optimization Approach
  Information Sciences (Partner: CERICT)

• Model-based Deployment of Secure Multi-cloud Applications
  International Journal of Grid and Utility Computing (Partners: CERICT, Tecnalia)

**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.
MUSA at Cloud Security Expo 2017

http://www.cloudexpoeurope.com/

MUSA actively participated 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 organised 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 were 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 also participated with:

- **Workshop** sessions that Cloud Watch 2 kindly supported, 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 was 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 SLA’s - Massimiliano Rak on MUSA innovations on Risk Analysis and security Service Level Agreement generation for (multi-)cloud-based applications. (15:15 - 15:40)

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.

MUSA at Cloud DevOps World 2017

https://tmt.knect365.com/cloud-devops-world/

Part of the TechXLR8, a big IT event, gathering more than 13K attendees, 8K companies, 800 speakers and 300 exhibitors, Cloud & DevOps World is oriented to cover all the key cloud innovations (containers, serverless, cloud native, security, DevOps approaches, etc.). The MUSA team presented the MUSA SecAP, targeting Chief Information Security Officers and IT administrators. Companies such as ENAC, FLYTECH, and ISKRATEL expressed their interest in the MUSA developments.
MUSA co-organised the SECPID Workshop at ARES Conference 2017

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

Under the umbrella of the Data Protection, Security and Privacy (DPSP) Cluster that MUSA coordinates, the project co-organised 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?

It is expected that next year MUSA will co-organize the SECPID 2018 too.

Paper submission deadline: April 15, 2017

MUSA co-organised the TAROT Summer School 2017

26 – 30 June, 2017, Naples, Italy.

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

As in 2016, this year the project organised 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 deadline: May 1, 2017.

MUSA participated at the IEEE SPC Workshop 2017

9-11 October, 2017, Las Vegas, NV USA.

http://cns2017.ieee-cns.org/content/technical-program

MUSA has been selected to be part of the European Commission’s Common Dissemination Booster (CDB), that offers free consultancy services to European, National, Regional funded Research &Innovation (R&I) projects (H2020, FP7 or other) aimed at improving the dissemination of results towards improving their exploitation. MUSA will participate in the CDB together with other nine EU-funded research projects from the Data Protection, Security and Privacy Cluster, working in areas related to MUSA topics: CREDENTIAL, PRISMACLOUD, SECURECLOUD, SERECA, SPECS, SUNFISH, SWITCH, TREDISEC, UNICORN.

Starting 29 January 2018, the group will participate in:

- Service 1: Portfolio Identification Service – Define portfolio of results and attributes in common across the cluster.
- Service 4: Portfolio Dissemination Capacity building – Learn the skills needed to improve your dissemination.
- Service 5: Dissemination Campaign in Practice – Hands-on support on delivering dissemination campaigns.

**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 YouTube channel**
https://www.youtube.com/channel/UCAmRopU82yKPhF5jkPSIPw

@MUSA_project (https://twitter.com/MUSA_project)

MusaProjectEU (https://www.facebook.com/MUSAProjectEU)