



## MULTI-cloud Secure Applications

<b>Data Management Report</b>	Deliverable ID:	D6.9
	Preparation date:	28/12/2017
	Editor/Lead beneficiary (name/partner):	Massimiliano Rak, Valentina Casola / CeRICT
	Internally reviewed by (name/partner):	Erkuden Rios / Tecnalia Antonio M. Ortiz / MI
Abstract: <p>This deliverable describes the policy adopted for the management of data produced during the project activity. This is the second release of the deliverable and supersedes the previous two (D6.3, D6.7). It describes the types of data the project generated/collected, which standards were used, how and in which cases the data were exploited, shared and/or made accessible to others, how the data were curated and preserved, even after the project duration.</p>		
<b>Dissemination level</b>		
<b>PU</b>	Public	X
<b>CO</b>	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 Tecnalía Research & Innovation  
(TECNALIA, Spain)  
[www.tecnalia.com/en](http://www.tecnalia.com/en)

**Project manager:** Erkuden Rios  
[erkuden.rios@tecnalia.com](mailto:erkuden.rios@tecnalia.com)  
+34 664 100 348



Centro Regionale Information e Communication Technology  
(CER ICT, Italy)

Contact: Massimiliano Rak  
[massimiliano.rak@unina2.it](mailto:massimiliano.rak@unina2.it)



CA Technologies Development Spain SAU (CA, Spain)

Contact: Victor Muntés  
[Victor.Muntes@ca.com](mailto:Victor.Muntes@ca.com)



Montimage  
(MI, France)

Contact: Edgardo Montes de Oca  
[edgardo.montesdeoca@montimage.com](mailto:edgardo.montesdeoca@montimage.com)



AIMES Grid Services  
(AIMES, UK)

Contact: Prof Dennis Kehoe  
[dennis.kehoe@aimes.net](mailto:dennis.kehoe@aimes.net)



Lufthansa Systems  
(LSY, Germany)

Contact: Dirk Bracklow  
[dirk.bracklow@lhsystems.com](mailto:dirk.bracklow@lhsystems.com)



TTY-säätiö  
(TUT, Finland)

Contact: José Luis Martínez Lastra  
[jose.lastra@tut.fi](mailto:jose.lastra@tut.fi)



## Table of contents

MUSA consortium .....	3
Table of contents .....	4
List of figures .....	6
List of tables .....	7
Executive summary .....	8
1 Introduction .....	9
1.1 Objective of the document .....	9
1.2 Structure of the document .....	9
1.3 Relationships with other deliverables .....	10
1.4 Contributors .....	10
1.5 Acronyms and abbreviations .....	10
1.6 Revision history .....	10
2 Expected Types of Data in MUSA .....	11
3 Scientific Publications .....	13
3.1 Scientific Publications Data Set Description .....	13
3.2 Standards and Metadata .....	13
3.3 Data Sharing.....	13
3.4 Access to MUSA Scientific Publications.....	13
3.5 Discover the MUSA Scientific Publications.....	13
3.6 Archiving and Preservation.....	14
4 Public Reports .....	15
4.1 Public Report Data Set Description .....	15
4.2 Standards and MetaData .....	16
4.3 Data Sharing.....	16
4.4 Access to MUSA Public Deliverables .....	16
4.5 Discover the MUSA Public Deliverables .....	16
4.6 Archiving and Preservation.....	16
5 Open Source Software.....	17
5.1 Open Source Software Data Set Description .....	17
5.2 Standards and MetaData .....	18
5.3 Data Sharing.....	18
5.4 Access to MUSA Open Source Software .....	18
5.5 Discover the MUSA Open Source Software.....	18
5.6 Archiving and Preservation.....	19
6 Public Videos .....	20
6.1 Public Videos Description .....	20
6.2 Standards and MetaData .....	20
6.3 Data Sharing.....	20
6.4 Access to MUSA Videos .....	21
6.5 Discover the MUSA Videos .....	21
6.6 Archiving and Preservation.....	21
7 Research Data.....	22
7.1 Research data Description.....	22
7.2 Standards and MetaData .....	22
7.3 Data Sharing.....	22
7.4 Access to MUSA Research Data .....	22
7.5 Discover the MUSA Research Data.....	22



---

7.6 Archiving and Preservation.....	23
References .....	24
Appendix A. MUSA motivation and background.....	25



## List of figures

Figure 1: DMP Life Cycle..... 9



## List of tables

Table 1: MUSA types of data available at M36 .....	11
Table 2: MUSA types of data.....	12
Table 3: Public deliverables at M36.....	15
Table 4: Open Source Repositories at M36.....	17
Table 5: Public Videos in MUSA Youtube channel at M36 .....	20



## Executive summary

This document describes the Final Data Management Plan (DMP) for the *Multi-cloud Security Applications* (MUSA) Project (see Appendix A). This is the third release of the DMP, during the project life cycle a new release of this deliverable has updated the previous DMP as described in Section 1. This third version supersedes the previous deliverable D6.7 *Data management report*, whose content is partially replicated in this document. D6.7 is *Obsolete* after the release date of this document.

This document describes the policy adopted for the management of data produced during the project activity. It describes the types of data the project has generated/collected, which standards have been used, how and in which cases the data have been exploited, shared and/or made accessible to others, and how the data will be curated and preserved, even after the project duration.

The document is structured as follows: the introductory Section 1 describes the DMP life cycle and explains the context of the document. Then, Section 2 gives an overview of the types of data managed in the project. Each of the following sections (Section 3, Section 4, Section 5, Section 6) is devoted to a type of data, describing the policies adopted for their management.





# 1 Introduction

## 1.1 Objective of the document

This document describes the *Multi-cloud Security Applications (MUSA) Project Data Management Plans (DMPs)*, as introduced in the Horizon 2020 Work Programme for 2014-15:

*“A further new element in Horizon 2020 is the use of Data Management Plans (DMPs) detailing what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research.”*

The MUSA DMP is a live document, updated during the project as illustrated in Figure 1, which assumes three (3) incremental releases of the DMPs, at months M6, M18 and M36 (end of project) respectively. The DMP addresses the management procedures for each types of data generated in the project. Similarly, the DMP description document, as also introduced in Section 1.2, contains a section for each type of data produced during the project.



**Figure 1: DMP Life Cycle**

Any new version of DMP will include all the information of the previous release, which will be considered obsolete from the release date of the new DMP, i.e., DMP released at M18 will contain all the sections of DMP release at M6. Note that if DMP released at M18 contains corrections to sections in common with M6, the policies described in the DMP released at M18 are valid for the remainder of the project.

Each release of the DMP, included the initial release, reports the management policies only for the data actually produced at the release date of the DMP. The first section after the introductory section reports the description of all the type of data that the MUSA project is expected to produce.

## 1.2 Structure of the document

The DMP contains an initial Section 2 that outlines the possible types of data produced by the project. For each type of data, a dedicated section describes the management policies; this release contains Section 0 devoted to Scientific Publications, Section 4 which describes Public Reports, Section 5 which describes the Open Source Software released by the project and Section 6, which describes the MUSA Videos describing the MUSA tools.

Each section devoted to a type of data contains:



- (i) a description of the type of data;
- (ii) a description of the standards adopted for that data and/or a description of their format (metadata);
- (iii) a description of the way in which such data are shared;
- (iv) a description of how to access to such data;
- (v) a description of how to discover such data;
- (vi) a description of the mechanisms used in the MUSA project to archive and preserve such data.

The document includes in Appendix A the overview of MUSA motivation and background, common to all MUSA deliverables.

### 1.3 Relationships with other deliverables

All deliverables affect indirectly this document, due to the data they contain. According to Section 1.2, this deliverable contains a section for each type of data produced by the project.

The following documents are directly related to D6.9:

- D6.3 *Data Management Plan* (M6) contains the initial version of the DMP, delivered at month 6.
- D6.7 *Data management report* (M18) contains the revised version of the DMP for MUSA project, delivered at month 18.

### 1.4 Contributors

All partners contributed to the definition of the policies adopted for the data management plan; CeRICT and Tecnalia are the main contributors of the deliverable.

### 1.5 Acronyms and abbreviations

DMP      Data management Plan

### 1.6 Revision history

Version	Date issued	Author	Organisation	Description
0.1	18/12/2017	Massimiliano Rak	CeRICT	Structure of the document, sections on publications, Public reports, Open source software, Videos
0.1.2	19/12/2017	Erkuden Rios	Tecnalia	Review 1
0.1.3	19/12/2017	Antonio M. Ortiz	MI	Review 2
0.2	28/12/2017	Massimiliano Rak	CeRICT	Final Revised
1.0	28/12/2017	Erkuden Rios	Tecnalia	Final Release



## 2 Expected Types of Data in MUSA

In order to classify the data types produced during the project, we focused on the description of the work and on the results obtained in the 36 months of the project.

According to such consideration, this section reports the data types produced during the whole project. Table 1 reports a brief description for each of them and few considerations related to the policies to be applied for each type of data. A complete section of DMP is dedicated for each data type reported in Table 1.

**Table 1: MUSA types of data available at M36**

Data Type	Description	Notes
<b>Scientific Publications</b>	Publications containing results of the project.	Scientific publications are subject to copyrights, depending on the editorial form they assume. DMP policies have to take into account both the need for large diffusion and the need for a well-evaluated editorial collocation.
<b>Public Reports</b>	MUSA public deliverables and eventual internal reports and whitepapers.	Eventual internal reports and whitepaper could be produced during the project. DMP rules outline how they are made publicly available.
<b>Open Source Software</b>	Software developed under Open source license and publicly made available at the end of the project.	Open source software was documented by deliverable and made available through public repositories.
<b>Research Data</b>	Data, which supports Scientific Publications and/or Public Reports for validation of results.	Annotated data of a corresponding type dependant on the context where data was captured (e.g., different types of logs, configuration files, etc.).
<b>Videos</b>	Public Videos documenting the MUSA results.	Videos documenting the project results through simple usage experiences and concrete examples and informative videos.

According to the work done in the first eighteen months of the project, we already identified a set of possible data types that have remained during the project lifetime. Table 2 reports such data types together with few considerations among them. Note that we removed the Multi-cloud application scenarios collected during the first year of the project as data set, because we considered them useful for the MUSA framework definition, but we agreed in not sharing them publicly.

Moreover, we added the Threat catalogue. Both Security Metric catalogue and Threat catalogue are currently in a joint database, the so-called MUSA Security Metrics Catalogue. Please refer to deliverable D2.1 *Initial SbD methods for multi-cloud applications* to learn on the metric format and contents in the catalogue. Deliverable D4.3 *Final security assurance mechanisms and tools* also includes a snapshot of the current MUSA Security Metrics Catalogue.

The public repository where the catalogue is available is here: <https://bitbucket.org/cerict/sla-model>



**Table 2: MUSA types of data**

Data Type	Description	Notes
<b>Research Data</b>	Data, which supports Scientific Publications and/or Public Reports for validation of results.	Annotated data of a corresponding type dependant on the context where data was captured (e.g., different types of logs, configuration files, etc.).
<b>Open Source Software</b>	Software produced during the project under open source license.	Consortium Agreement describes the ownership rules for the code. DMP policies should only describe how the code is made publicly available if there is such an interest.
<b>Security Metrics Catalogue</b>	Security Metrics used in the project.	MUSA framework focuses on security aspects for multi-cloud applications. Security metrics are a known research topic and any contribution to collect standard quantifiable metrics is of interest for the project.
<b>Cloud Threats Catalogue</b>	Catalogue of Threats and risks in Cloud.	<p>The MUSA framework supports tools that simplify risk analysis in the cloud, in order to generate Security SLAs.</p> <p>Cloud Security Threats, together with detailed information that helps to identify when such threats apply, are being collected and made available to the community.</p> <p>Any contribution to enlarge such Threat Catalogue is of interest for the project.</p>
<b>Videos</b>	Public Videos on YouTube	MUSA documented many of the obtained results through videos made publicly available in MUSA YouTube channel.

## 3 Scientific Publications

### 3.1 Scientific Publications Data Set Description

This data set contains all the Scientific Publications developed in the project for the promotion of all the MUSA results. The full list of publications produced during the 36 months of the project is available in D6.8 (public report).

### 3.2 Standards and Metadata

Each MUSA Scientific Publication has followed the template that is specified in the publication procedures of the different conferences, books or journals where the publications were presented.

### 3.3 Data Sharing

The MUSA project has supported the open access approach to Scientific Publication (as defined in article 29.2 of the Grant Agreement). Scientific Publications covered by an editorial copyright have been made available internally to the partners and shared publicly through references to the copyright owners web sites.

Whenever possible, a Scientific Publication, as soon as possible and at the latest six months after the publication time, will be deposited in a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a repository for scientific publications. Moreover, the beneficiary should aim at depositing at the same time the research data needed to validate the results presented in the deposited scientific publications.

TECNALIA has published in *TECNALIA Publications* [3] open access repository. The repository fulfils international interoperability standards and protocols to gain long-term sustainability and feeds which feed RECOLECTA [4], a platform which gathers all scientific repositories at Spanish national level, and OpenAire [5], the EU open access platform for H2020 EU funded-projects' scientific publications.

All scientific publications of the MUSA project will be available through OpenAire repository and the potential delayed access ('embargo periods') required by specific publishers and magazines will be negotiated in a case-by-case basis.

The access to MUSA in OpenAire is:

[https://www.openaire.eu/search/project?projectId=corda\\_h2020::e88e39d049e0c7c858912c1cf6e49f45](https://www.openaire.eu/search/project?projectId=corda_h2020::e88e39d049e0c7c858912c1cf6e49f45)

### 3.4 Access to MUSA Scientific Publications

MUSA Scientific Publications will have open access to the deposited publication — via the repository — at the latest:

- on publication, if an electronic version is available for free via the publisher, or
- within six months of publication (twelve months for publications in the social sciences and humanities) in any other case.

### 3.5 Discover the MUSA Scientific Publications

For MUSA Scientific Publications, the open access has been ensured, via the repository, to the bibliographic metadata that identifies the deposited publications. The bibliographic metadata must be in a standard format and must include all of the following:

- the terms "European Union (EU)" and "Horizon 2020";
- the name of the action, acronym and grant number;
- the publication date, and length of embargo period if applicable, and



- a persistent identifier.

### 3.6 Archiving and Preservation

Scientific publications repositories increase visibility (and therefore the impact) of the work of the authors and the organisations to which they belong, using standardized international protocols that guarantee the visibility of documents in the search engines. These same protocols allow metadata of the repository and files within to be collected by external systems (collectors) to offer new services (e.g., search across multiple repositories, etc.). TECNALIA has made available the Tecnalia papers in *TECNALIA Publications* [3] repository which is an open access repository feeding RECOLECTA [4] and OpenAire [5], as explained before. The *TECNALIA Publications* repository is visible through Google and fulfils international interoperability standards and protocols to gain long-term sustainability. According to the aim of the consortium, as soon as they are reported to the European Commission, all public scientific publications of the MUSA project will be available through OpenAire repository which allows searching publications per project. The potential delayed access ('embargo periods') required by specific publishers and magazines will be negotiated in a case-by-case basis.



## 4 Public Reports

MUSA has produced as an open set of data a number of reports, which summarize the main projects activities and deliverables, marked as public.

The project deliverables will be released publicly, when it is prescribed in the description of the work, only after the acceptance from the European Commission. Internal reports and whitepapers have been made available publicly according to an agreement among the report authors.

### 4.1 Public Report Data Set Description

The following table shows the Public Deliverables at month 36 of the project. It is worth noticing that period 2 (M19-M36) deliverables are available and will be made publicly available as soon as they get the EC approval.

**Table 3: Public deliverables at M36**

Deliverable (number)	Deliverable name	Work package number	Due delivery month
D1.1	Initial MUSA framework specification.	WP1	M12
D1.2	Guide to security management in multi-cloud applications lifecycle.	WP1	M15
D1.3	Initial MUSA framework implementation.	WP1	M23
D1.4	Final MUSA framework specification and guide.	WP1	M35
D1.5	Final MUSA framework implementation.	WP1	M35
D2.1	Initial SbD methods for multi-cloud applications.	WP2	M15
D2.2	Initial MUSA IDE for security-aware design of multi-cloud applications	WP2	M23
D2.3	Final SbD methods for multi-cloud applications	WP2	M33
D2.4	Final MUSA IDE for security-aware design of multi-cloud applications	WP2	M33
D3.1	Initial security based discovery and composition mechanisms and tools	WP3	M23
D3.2	Initial secure multi-cloud deployment mechanisms and tools	WP3	M23
D3.3	Final security based discovery and composition mechanisms and tools	WP3	M35
D3.4	Final secure multi-cloud deployment mechanisms and tools	WP3	M35
D4.1	Initial security assurance mechanisms and tools	WP4	M23
D4.2	Initial MUSA Security Assurance Platform	WP4	M23
D4.3	Final security assurance mechanisms and tools	WP4	M35
D4.4	Final MUSA Security Assurance Platform and user manual	WP4	M35
D5.1	MUSA case studies work plan	WP5	M12
D5.3	Results of first evaluation of MUSA framework.	WP5	M24
D5.5	Results of final evaluation of MUSA framework	WP5	M36
D6.1	MUSA brochure and public website	WP6	M4
D6.2	Dissemination Strategy	WP6	M6
D6.3	Data Management Plan	WP6	M6
D6.4	Communication Plan	WP6	M6
D6.5	Networking plan	WP6	M9
D6.6	Dissemination, communication and networking report	WP6	M18
D6.7	Data management report	WP6	M18



D6.8	Final dissemination, communication, and networking report	WP6	M36
D6.9	Final data management report	WP6	M36
D7.1	Initial market study, trends, segmentation and requirements	WP7	M6
D7.2	Business scenarios analysis	WP7	M12
D7.5	Standards analysis and strategy plan	WP7	M6
D7.6	Revised standards strategy plan	WP7	M18
D7.7	Standards adoption report	WP7	M36

## 4.2 Standards and MetaData

MUSA Public Deliverables have a standard template available on the internal document management system (<https://intranet.musa-project.eu>). The Executive summary, at the beginning of the document is a brief summary of the deliverable content. All the information about the document is reported in Section 1 (Introduction).

All Introduction sections contain:

- A description of the objective of the deliverable (Section 1.1).
- A description of the structure of the deliverable (Section 1.2).
- A description of relationships with other deliverables (Section 1.3).
- A list of contributors (Section 1.4).
- A section devoted to summarize acronyms and abbreviations (Section 1.5).
- A section that reports the revision history (Section 1.6).
- A section that describes the changes applied in different versions after evaluation of the Commission (Section 1.7) - optional

## 4.3 Data Sharing

All public report/deliverables will be published through the MUSA website [1], in which there is a section where all the MUSA Public Results will be published and made available for free to the general public. All period 1 Public Results are already available and period 2 Public Results will be published as soon as they get the approval from the European Commission.

## 4.4 Access to MUSA Public Deliverables

The access to the public repository has been done through the Public Results section of the MUSA website [1].

For accessing to these public reports no identification is required.

## 4.5 Discover the MUSA Public Deliverables

The MUSA website [1] has been made as visible as possible and discovering is possible through any web search engine.

## 4.6 Archiving and Preservation

All final versions of the deliverables are maintained on the internal document management system (<https://intranet.musa-project.eu>), based on Alfresco. All reports available on the website are archived together with web site infrastructure (see D6.1 *MUSA brochure and public website*).





## 5 Open Source Software

MUSA has produced, as an open set of data, a number of software pieces developed adopting open source criteria.

The project open source code was released publicly at the end of the project, using free hosting by BitBucket (<http://bitbucket.org>).

### 5.1 Open Source Software Data Set Description

Table 4 shows the list of open source repositories produced by the MUSA project (including as well repositories forked and extended from other projects) and available from the end of the project.

**Table 4: Open Source Repositories at M36**

Name	Description	link
Modeller	Repositories hosting the Modeller tool code	<a href="https://bitbucket.org/musateam/eu.musa.modeller.web-tomcat">https://bitbucket.org/musateam/eu.musa.modeller.web-tomcat</a>
		<a href="https://bitbucket.org/musateam/eu.musa.modeller.ws">https://bitbucket.org/musateam/eu.musa.modeller.ws</a>
		<a href="https://bitbucket.org/musateam/eu.musa.modeller.utils">https://bitbucket.org/musateam/eu.musa.modeller.utils</a>
		<a href="https://bitbucket.org/musateam/org.camel_dsl.dsl.parent">https://bitbucket.org/musateam/org.camel_dsl.dsl.parent</a>
		<a href="https://bitbucket.org/musateam/org.camel_dsl">https://bitbucket.org/musateam/org.camel_dsl</a>
Dashboard and Risk Analysis	Repositories hosting the code of MUSA Dashboard, Risk Analysis and CSP Selection tools	<a href="https://bitbucket.org/musateam/musa-risk_assessment-excel_importer">https://bitbucket.org/musateam/musa-risk_assessment-excel_importer</a>
		<a href="https://bitbucket.org/musateam/musa-kanban-webserver">https://bitbucket.org/musateam/musa-kanban-webserver</a>
SLA Generation	Repositories hosting the code of the SLA Generation tool	<a href="https://bitbucket.org/cerict/sla-generator-v2">https://bitbucket.org/cerict/sla-generator-v2</a>
		<a href="https://bitbucket.org/cerict/sla-model">https://bitbucket.org/cerict/sla-model</a>
		<a href="https://bitbucket.org/cerict/specs-core-sla_platform-sla_manager">https://bitbucket.org/cerict/specs-core-sla_platform-sla_manager</a>
		<a href="https://bitbucket.org/cerict/specs-core-sla_platform-sla_manager-api">https://bitbucket.org/cerict/specs-core-sla_platform-sla_manager-api</a>
SLA Composition Framework	Repositories hosting the development framework for the SLA composition process	<a href="https://bitbucket.org/cerict/securitycontrolgraphs">https://bitbucket.org/cerict/securitycontrolgraphs</a>
MUSA Deployer	Repositories hosting the code of the MUSA Deployer	<a href="https://bitbucket.org/musateam/musa-deployer">https://bitbucket.org/musateam/musa-deployer</a>
		<a href="https://bitbucket.org/cerict/musa-deployer">https://bitbucket.org/cerict/musa-deployer</a>



		<a href="https://bitbucket.org/cerict/musa-external-repository">https://bitbucket.org/cerict/musa-external-repository</a>
		<a href="https://bitbucket.org/cerict/musa-applications-repository">https://bitbucket.org/cerict/musa-applications-repository</a>
MUSA Assurance Platform	Repositories hosting the code of the MUSA Security Assurance Platform	<a href="https://bitbucket.org/musateam/musa-assurance_platform-behaviour_agent">https://bitbucket.org/musateam/musa-assurance_platform-behaviour_agent</a>
		<a href="https://bitbucket.org/musateam/musa-assurance_platform-agents">https://bitbucket.org/musateam/musa-assurance_platform-agents</a>
		<a href="https://bitbucket.org/musateam/musa-assurance_platform">https://bitbucket.org/musateam/musa-assurance_platform</a>
		<a href="https://bitbucket.org/musateam/musa-assurance_platform-monitoring_agent">https://bitbucket.org/musateam/musa-assurance_platform-monitoring_agent</a>
		<a href="https://bitbucket.org/musateam/musa-assurance_platform-enforcement">https://bitbucket.org/musateam/musa-assurance_platform-enforcement</a>
		<a href="https://bitbucket.org/musateam/musa-assurance_platform-enforcement_agents">https://bitbucket.org/musateam/musa-assurance_platform-enforcement_agents</a>

## 5.2 Standards and MetaData

The MUSA Open Source software are published accordingly to the Bitbucket templates and accordingly to the type of code developed. The MUSA Repositories have their own readme file that gives the information needed to access to the software documentation. Public Deliverables document the software.

## 5.3 Data Sharing

All MUSA Open Source software has been published on the open source repositories and diffused through the MUSA website [1]. In the website of MUSA project there is a section for MUSA tools where all the MUSA Open Source repositories links are collected.

## 5.4 Access to MUSA Open Source Software

The MUSA Open Source Software Repositories allow direct access from public, enabling code forks (keeping trace of the forks). Owners' teams will maintain administrative rights over the repositories in order to enable access to code and enrolment of developers even after the MUSA project.

## 5.5 Discover the MUSA Open Source Software

The MUSA website [1] will maintain the direct links to the MUSA Open Source Software Repositories. Bit Bucket offer search engines among the maintained repositories.

Each team will diffuse the links to the maintained repositories among the interested communities.



## 5.6 Archiving and Preservation

All Open source software were published over public repositories maintained by the owners' teams on Bitbucket (<http://bitbucket.org>) even after the end of the project.



## 6 Public Videos

MUSA has produced, as an open set of data, a number of videos documenting the MUSA results. The MUSA videos were publicly released on YouTube through a dedicated **MUSA project Youtube channel** (<https://www.youtube.com/channel/UCA7mR0pU82yKPhF5jkPSIPw>) and their links are diffused through the MUSA website [1].

### 6.1 Public Videos Description

¡Error! No se encuentra el origen de la referencia. shows the list of Videos produced by MUSA project (including even repositories forked and extended from other projects) and available from the end of the project. It is worth noticing that the consortium may update the channel even after the end of the project adding new videos, in order to help post-project dissemination activities. Please note that the videos named with “New” correspond to final versions of the tools integrating the MUSA framework, and therefore supersede initial versions.

**Table 5: Public Videos in MUSA Youtube channel at M36**

Video
MUSA
MUSA Showcases
MUSA Dashboard
New MUSA Dashboard
MUSA Modeller
New MUSA Modeller
MUSA Risk Assessment & Services Selection
MUSA Decision Support Tool
MUSA SLA Generator (proof-of-concept)
MUSA SLA Generation (v2)
MUSA Deployment Plan and Execution
New MUSA Deployment Plan and Execution
MUSA Deployer Broker
MUSA Security Assurance Platform demo
New MUSA Security Assurance Platform Monitoring
New MUSA Security Assurance Platform Enforcement

### 6.2 Standards and MetaData

MUSA Videos are available on YouTube and can be accessed through any browser web.

### 6.3 Data Sharing

All Videos are published on the MUSA EU project channel, available at the link <https://www.youtube.com/channel/UCA7mR0pU82yKPhF5jkPSIPw>.

The Videos are also reachable at the MUSA public website [www.musa-project.eu](http://www.musa-project.eu) within Tools menu.



## **6.4 Access to MUSA Videos**

The MUSA YouTube channel and the MUSA Videos are publicly available to any user.

## **6.5 Discover the MUSA Videos**

The MUSA website [1] will maintain the direct links to the MUSA Videos.

The MUSA Videos can be found through the YouTube and Google searching services.

Each team will diffuse the links to the Videos among the interested communities.

## **6.6 Archiving and Preservation**

All Videos will be maintained on the MUSA YouTube channel even after the end of the project. The Project Coordinator, the WP6 leader and the Dissemination Leader will maintain the MUSA YouTube channel administrative credentials even after the end of the project, even if no new Videos will be added.



## 7 Research Data

MUSA has produced a large set of research data, though some of them (like SLAs of software components and CSPs) cannot be released as open data, because they are under ownership of third parties and/or contain confidential data of partners, other, like the metric and the threat catalogues are made publicly available.

### 7.1 Research data Description

The open research data produced in MUSA are: The Security Metric Catalogue and the Threat Catalogue.

The Security Metric Catalogue, which is the result of a shared effort with other projects (e.g. SPECS and A4Cloud), is a collection of security metrics that are (i) extracted from standard documents (like NIST and CIS publications), (ii) extracted from scientific publications or (iii) defined in the context of the projects. The catalogue collects for each security metric the name, the definition, the original source of the metric definition, and suggests the security controls that can be directly and/or indirectly measured through the metric.

The Threat Catalogue was produced specifically inside the MUSA project and it collects a large set of threats, extracted by (i) open data collections like Mitre CVW/CWE/CAPEC lists, WASC or Vulnerabilities databases, (ii) list of top threats produced by security consortium (e.g. CSA) and public security entities (like CERTs or ENISA) or (iii) scientific publications. The catalogue collects for each threat the name, the definition, the original source of the threat identification a set of information useful for risk rating (e.g. threat agent skills, impact in terms of confidentiality, integrity or availability, ...), the STRIDE classification of the threat and suggested countermeasures, in terms of standard security controls.

A complete and detailed description of the Metric Catalogue and of the Threat Catalogue was produced in deliverables D2.1 *Initial SbD methods for multi-cloud applications* and D2.3 *Final SbD methods for multi-cloud applications*.

### 7.2 Standards and MetaData

Both the catalogues are offered as a single relational database, together with a tool able to automatically generate the data and store them in a MySQL DB. The details on the data model are available in D2.3, Section 5 (public report).

### 7.3 Data Sharing

The software to generate the catalogues relational database and the backup of the Catalogues DB to make a manual restore of the database are available in the open source sla-model repository (<https://bitbucket.org/cerict/sla-model>). The Repository readme contains all the information needed to download the DB and/or to use the tool to automatically generate it.

### 7.4 Access to MUSA Research Data

The Catalogues are available as open source repositories and are publicly available to any user.

### 7.5 Discover the MUSA Research Data

The MUSA website [1] will maintain the direct links to the MUSA Repositories.

The MUSA research data can be found through the Atlassian indexing on bitbucket and using Google searching services.

Each team will diffuse the links to the data repositories among the interested communities.



## 7.6 Archiving and Preservation

All Data catalogues will be maintained on the bitbucket repository even after the end of the project.



## References

- [1] MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017. Available at: [www.musa-project.eu](http://www.musa-project.eu)
- [2] Workshop on Security and Privacy in Systems and Communication Networks, SecureSysComm 2015. Available at: <http://wpage.unina.it/ficco/SecureSysComm2015/home.html>
- [3] TECNALIA Publications by TECNALIA. Available at: <http://dsp.tecnalia.com/>
- [4] RECOLECTA by FECYT. Available at: <http://recolecta.fecyt.es/portada?language=es>
- [5] OpenAire H2020 Project. Available at: <https://www.openaire.eu/>

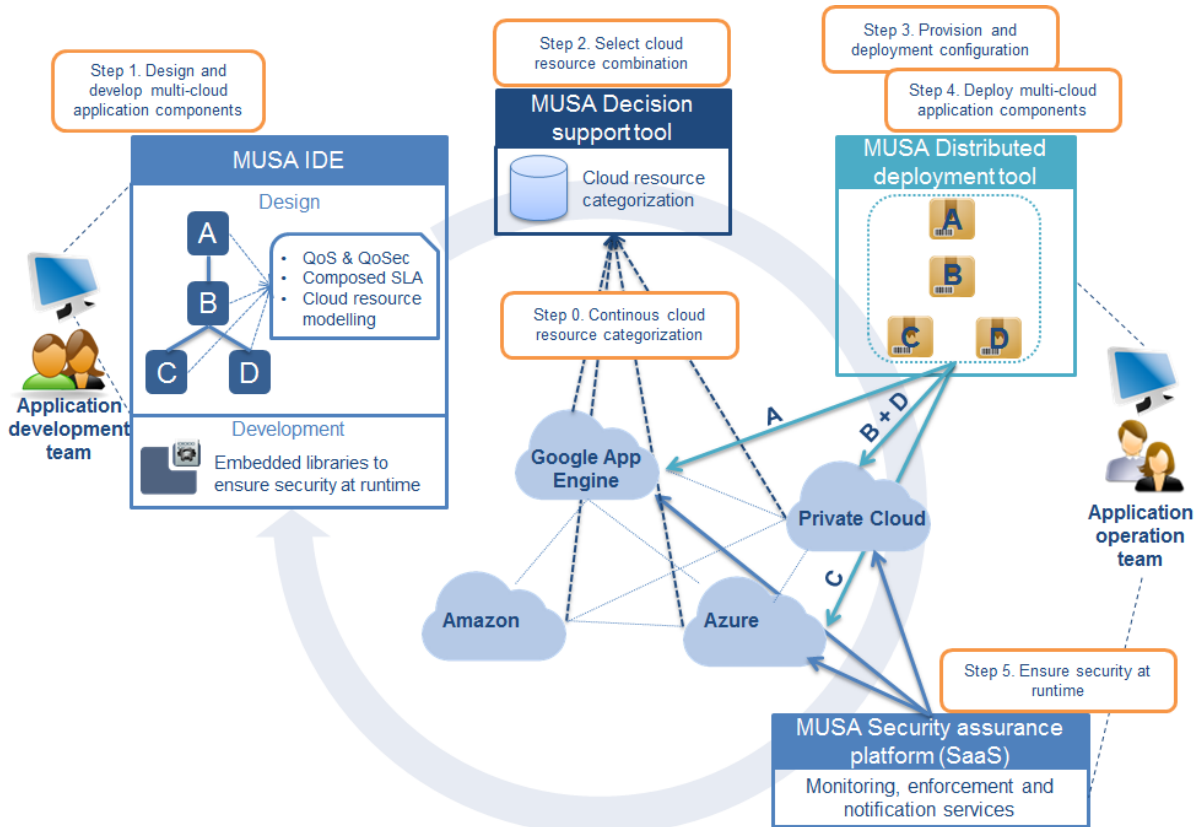




## Appendix A. MUSA motivation and background

The main goal of MUSA project<sup>1</sup> 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: 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.

<sup>1</sup> MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017, <http://www.musa-project.eu>

