MUlti-cloud Secure Applications

Deliverable title	Deliverable ID: D6.3
	Preparation date: 30/06/2015
Data Management Plan	Editor/Lead beneficiary (name/partner): Massimiliano Rak, Valentina Casola / CeRICT
	Internally reviewed by (name/partner): Andrei Lobov / TUT Victor Muntes / CA

Abstract:

This deliverable describes the policy adopted for the management of data produced during the project activity. It described the types of data the project will generate/collect, which standard will be used, how and in which cases the data will be exploited, shared and/or made accessible to others, how the data will be curated and preserved, even after the project duration.

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

The project leading to this work 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 Muntés 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

This document describes the Data Management Plan (DMP) for the *MUlti-cloud Security Applications* (MUSA) Project (see Appendix A). This is the first release of the DMP, during the project life cycle new release of this deliverable will update the DMP as described in Section 1.

This document describes the policy adopted for the management of data produced during the project activity. It describes the types of data the project will generate/collect, which standard will be used, how and in which cases the data will be 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 expected type of data to be managed. Each of the following sections (Section 3 and Section 4) is devoted to a type of data, describing the policies adopted for their management.

1 Introduction

1.1 Purpose 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 four (4) incremental releases of the DMPs, at months M6, M18, M30 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, will contain a section for each type of data produced during the project.

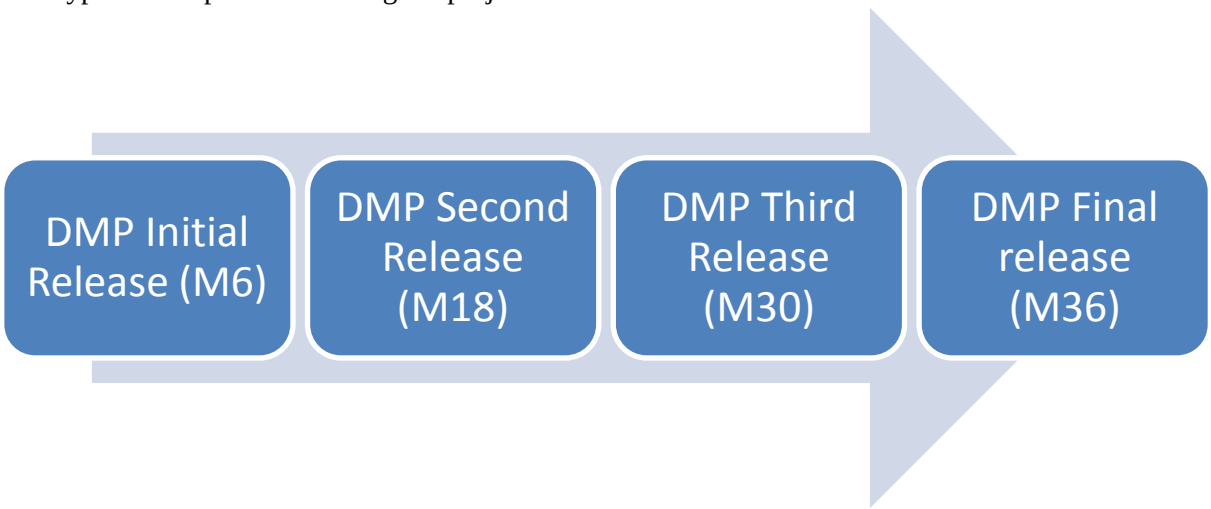

Figure 1: DMP Life Cycle

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 section 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, will report the management policies only for the data actually produced at the release date of the DMP. The first section after the introductory section will report 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 3, devoted to Scientific Publications and Section 4, which describes Public Reports.

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.

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.

The following documents are directly related to D6.3:

- D6.6 *Dissemination, communication, networking and data management report* (M18) will contain the revised version of the DMP at month 18.
- D6.7 *Final dissemination, communication, networking and data management report* (M36) will contain the final version of the DMP for MUSA project.

1.5 Acronyms and abbreviations

DMP Data management Plan

1.6 Revision history

Version	Date issued	Author	Organisation	Description
0.1	15/04/2015	Massimiliano Rak	CeRICT	Structure of the document, sections on Public deliverable, Open source software, multi-cloud application scenarios, security metrics catalogue
0.2	13/05/2015	Marisa Escalante	Tecnalia	Added Scientific publication section, removed for this version open source software, multi-cloud application scenarios, security metric catalogue
0.3	18/06/2015	Massimiliano Rak	CeRICT	Updated All description, finalized the draft version.

Version	Date issued	Author	Organisation	Description
2.0	25/06/2015	Massimiliano Rak	CeRICT	Final proposed version
2.1	28/06/2015	Massimiliano Rak	CeRICT	Final revised
2.2	29/06/2015	Erkuden Rios	Tecnalia	Final review pre-release
2.3	30/06/2015	Erkuden Rios	Tecnalia	Final released

1.7 Change log

No change log entries.

2 Expected Types of Data in MUSA

In order to collect the data types that will be produced during the project, for this first release of DMP, we focused on the description of the work and on the results obtained in the first months of the project.

According to such consideration, this section **¡Error! No se encuentra el origen de la referencia.** reports the data type produced during the first months of the project. Table 1 reports a very 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 **¡Error! No se encuentra el origen de la referencia.**.

Table 1: MUSA types of data available at M6

Data Type	Description	Notes
Scientific Publications	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.
Public Reports	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.
Research Data	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.).

According to the work done in the first six months of the project, we already identified a set of possible data types that will be made available in the next releases of DMP. The following Table 2**¡Error! No se encuentra el origen de la referencia.** reports such data types together with few considerations among them.

Table 2: MUSA expected types of data

Data Type	Description	Notes
Research Data	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.).
Open Source Software	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.
Multi-cloud Application Scenarios	Description of multi-cloud scenarios.	MUSA framework focuses on a class of applications (e.g. multi-cloud application), which are new at state of art. Collection of scenarios is of interest for

		the cloud community in order to well define the multi-cloud problem.
Security Metrics Catalogue	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.

3 Scientific Publications

3.1 Scientific Publications Data Set Description

This data set will contain all the Scientific Publications developed in the project for the promotion of all the MUSA results.

In the first 6 months of the project, the following Scientific Publications have been developed:

- "Towards Self-Protective Multi-Cloud Applications MUSA – a Holistic Framework to Support the Security-Intelligent Lifecycle Management of Multi-Cloud Applications". Written by Erkuden Rios, Eider Iturbe, Leire Orue-Echevarria, Massimiliano Rak and Valentina Casola. Presented in CLOSER 2015 "5th International Conference on Cloud Computing and Services Science" http://closer.scitevents.org/Home.aspx.

In addition the publications are prepared for the Workshop on Security and Privacy in Systems and Communication Networks 2015 [2].

3.2 Standards and Metadata

Each MUSA Scientific Publication will follow the template that is asked in the publication procedures of the different conferences, books or publications where the publications will be presented.

3.3 Data Sharing

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

Whenever is 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 just finalised the development of its own repository which is accessible by RECOLECTA [3] (a platform which gathers all scientific repositories at Spanish national level) and OpenAire [4] (a new platform aimed at gathering a H2020 EU funded-projects' scientific publications). The repository fulfils international interoperability standards and protocols to gain long-term sustainability.

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.

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, it will be ensured open access, via the repository, to the bibliographic metadata that identify the deposited publication. 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 can be collected by external systems (collectors) to offer new services (e.g. search across multiple repositories, etc.). TECNALIA has just finalised the development of the *TECNALIA Publications* repository which is an open access repository accessible by RECOLECTA [3] and OpenAire [4] as explained before. The *TECNALIA Publications* repository is visible through Google and fulfils international interoperability standards and protocols to gain long-term sustainability.

The aim of the consortium is that all 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 produces 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 will be 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 6 of the project.

Table 3: Public deliverables at M6

Deliverable (number)	Deliverable name	Work package number
D6.1	MUSA brochure and public website	WP6
D6.2	Dissemination Strategy	WP6
D6.3	Data Management Plan	WP6
D6.4	Communication Plan	WP6
D7.1	Initial market study, trends, segmentation and requirements	WP7
D7.5	Standards analysis and strategy plan	WP7

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 purpose 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 the website of MUSA project there is a section where all the MUSA Public Results will be published and made available for free to the general public.

4.4 Access to MUSA Public Deliverables

The access to the public repository will be done through the Public Results section of the MUSA website.

For accessing to these public reports no identification is going to be required.

4.5 Discover the MUSA Public Deliverables

The MUSA website will be made as visible as possible and discovering should be 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 web site are archived together with web site infrastructure (see D6.1 *MUSA brochure and public website*).

References

[1] MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017. Available at: 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] RECOLECTA by FECYT. Available at: http://recolecta.fecyt.es/portada?language=es

[4] OpenAire H2020 Project. Available at: https://www.openaire.eu/

Appendix A. MUSA motivation and background

The main goal of MUSA project[1] 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.

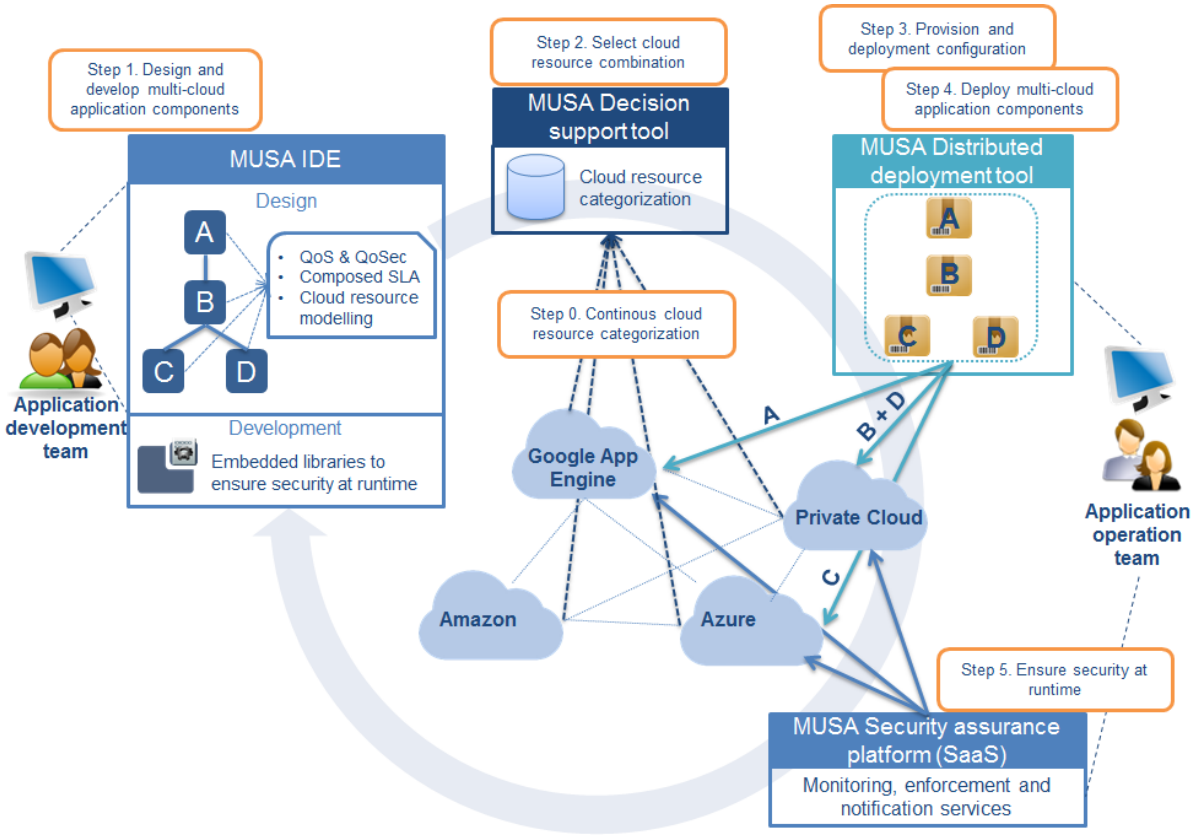

Figure: MUSA overall concept

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.

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