



MUlti-cloud Secure Applications

Standards Analysis and Strategy Plan	Deliverable ID:	D7.5
	Preparation date:	30/06/2015
	Editor/Lead beneficiary (name/partner):	Peter Matthews / CA
	Internally reviewed by (name/partner):	Antony Shimmin / AIMES Antonio Ortiz / Montimage
Abstract: This deliverable presents the most relevant standards identified for the MUSA solution and the designed strategy for their adoption and inclusion in MUSA.		
Dissemination level		
PU	Public	X
CO	Confidential, only for members of the consortium and the Commission Services	



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

MUSA consortium



Fundación Tecnalía 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 Munes
Victor.Munes@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@ames.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

MUSA consortium	3
Table of contents	4
List of figures	5
List of tables	6
Executive summary	7
1 Introduction	9
1.1 Purpose of the document.....	9
1.2 Structure of the document	9
1.3 Relationships with other deliverables	9
1.4 Contributors	9
1.5 Acronyms and abbreviations.....	9
1.6 Revision history	10
2 Introduction to Cloud computing standards landscape.....	11
3 Adoption of standards within MUSA.....	12
3.1 Standards for multi-cloud application modelling.....	13
3.1.1 CloudML	13
3.1.2 TOSCA	13
3.1.3 OCCI.....	13
3.1.4 CAMP.....	13
3.2 Standards for multi-cloud application security requirements specification in SLA	14
3.2.1 WS Agreement	14
3.2.2 SUoM	15
3.3 Standards for Cloud computing service metrics	15
3.3.1 NIST Cloud Reference Architecture (NIST 500-292).....	15
3.3.2 ISO Cloud SLA framework (ISO/IEC NP 19086)	15
3.3.3 CSA	15
3.4 Related organisations and initiatives.....	15
3.4.1 EC CSIG	15
3.4.2 CSA	16
3.4.3 CSCC.....	16
3.4.4 MPAA.....	16
3.4.5 ENISA guidelines on cloud security.....	16
3.4.6 CloudWatch works on cloud security.....	18
3.5 Standards and best practices planned for adoption in MUSA.....	19
3.6 Additional standards under observation.....	20
3.7 Plan for Adoption of Standards in MUSA framework.....	21
4 Impact of MUSA on standards	23
4.1 The role of the consortium in developing and emerging standards	23
4.2 Influence on standards	23
5 Conclusions	24
References	25
Appendix A. MUSA motivation and background.....	29



List of figures

Figure 1: Plan for adoption of standards 22



List of tables

Table 1: ETSI CSC identified standards	11
Table 2: Summary of existing standards related to MUSA research topics	12
Table 3: Cloud Certification Schemes List	17
Table 4: Initial list of standards and best practices for adoption	20
Table 5: Other standards under observation of MUSA	20



Executive summary

Maintenance of interoperability between components and applications is simpler to achieve if the use of recognised de-facto and de-jure standards are used. This document reviews standards that are current or under development in the field of cloud computing and cloud based services. Standards and strategy are considered in the following sections. These sections describe the process for adoption of standards, some of the standards that are likely to be adopted, and discusses the use of best practices to complement the project in areas where there are no standards or where standards do not apply. Appendix A gives the background information about the project.

Standards and the work of the MUSA project are evolving. For this reason the strategy for adoption and influencing standards is based on a continual review of emerging standards as well as the potential for applying them to the evolving MUSA framework. As such the project will use a standards observatory approach and review standards and emerging standards. This involves a regular scan of the standards bodies and discussions with members of standards technical committees and working groups.





1 Introduction

1.1 Purpose of the document

The present document, *D7.5 Standards Analysis and Strategy Plan*, is the first deliverable of the standardisation task in MUSA project (see Appendix A). The deliverable includes the analysis of the relevant standards for the MUSA research as well as the standardisation strategy plan of the project. The strategy plan outlines the impact of standardisation on the project and the plan to enhance or develop further standards in the area of multi-cloud security management.

1.2 Structure of the document

The document is structured as follows. After this introductory section, Section 2 provides an overview of the Cloud computing standardisation landscape. Then, Section 3 describes the standards as well as the organisations and initiatives relevant for MUSA project (Sections 3.1 to 3.6). It also details the plan for the adoption of standards within the project (Section 3.7). Section 4 explains how MUSA intends to impact on standards. Finally, Section 5 concludes the document and indicates future intended work. The Appendix A summarizes the MUSA project motivation and background.

1.3 Relationships with other deliverables

The present deliverable relates to the following future deliverables of the project:

- *D7.6 Revised standards strategy plan*, M18: This report will revise the present document and describe the progress of the adoption of the different standards within MUSA tools and methods and may also analyse other additional standards that may have appeared in the context of the project so as to define the strategy to include them in MUSA.
- *D7.7 Standards adoption report*, M36: This report will rely on the decisions taken to adopt or not the different standards. Depending on the relevancy of the obtained results, the consortium will evaluate the necessity of performing liaison activities with standardisation bodies for proposing a potential extension

1.4 Contributors

The following partners have contributed to this deliverable:

- CA
- TECNALIA
- CERICT

1.5 Acronyms and abbreviations

CAMP	Cloud Application Management for Platforms (OASIS)	ODCA	Open Data Centre Alliance
CCM	Counter with CBC-MAC	OGF	Open Grid Forum
CSA	Cloud Security Alliance	SLA	Service Level Agreement
CSCC	Cloud Standards Customer Council	SMI	Service Measurement Index
ENISA	European Network and Information Agency	SUoM	Standard Units of Measure
ISO	International Organisation for Standardisation	TMF	TM Forum
MPAA	Motion Picture Association of America	TOSCA	Topology and Orchestration Specification for Cloud Applications
NIST	National Institute for standards and technology	W3C	World Wide Web Consortium



1.6 Revision history

Version	Date issued	Author	Organisation	Description
0	22 nd Apr 2015	Peter Matthews	CA	Initial Document format and ToC
1	28 th Apr 2015	Peter Matthews	CA	Moved section 1.1 text to Appendix and created initial entries for executive summary, Cloud Standards Landscape and Approach
2	6 th May 2015	Peter Matthews	CA	Completed work on standards influence and adoption
3	8 th May 2015	Erkuden Rios	Tecnalía	Contributed to Sections 1, 2, 3 and 4.
4	18 th May 2015	Peter Matthews	CA	Updated figure 1, completed description of adoption process Completed Executive Summary
5	28 th May 2015	Peter Matthews	CA	Incorporated CeRICT contributions and completed sections on CloudML, Adopted Standards and Conclusion
6	22 nd June 2015	Peter Matthews	CA	Final edits for last review before issue
7	25 th June 2015	Peter Matthews	CA	Edits from Antonio review
8	26 th June 2015	Erkuden Rios	Tecnalía	Edits to improve formats, references and all sections' contents.
9	29 th June 2015	Peter Matthews	CA	Edits after Erkuden review
1.0	30 th June 2015	Erkuden Rios	Tecnalía	Final released.

2 Introduction to Cloud computing standards landscape

Since cloud services moved outside the organisations boundaries there has been a lot of interest in standards as a means of ensuring interoperability and portability. Cloud computing standards were suspected to be very patchy and incomplete in many areas, however there are a number of initiatives that are trying to create a cleared picture.

The most recent European initiative is the one started in December 2012 by the European Commission within its Cloud Strategy Key action 1 *Cutting through the jungle of Standards*. The EU Commission requested ETSI standardisation body to study the landscape of Cloud standards and identify the gaps to support the policy objectives defined by the European Commission.

ETSI Cloud Standards Coordination (CSC) group [1] completed its Phase 1 report in November 2013. This document takes use cases to define requirements that are matched with standards. The Table 1 below refers to some of the conclusions of CSC work in Phase 1 and while some of these may be out of date indicate that in many areas of Cloud computing there are few or no specific standards but existing computing standards may be applicable.

In February 2015, CSC Phase 2 was launched to address issues left open after CSC Phase 1, with the objective to *investigate some specific aspects of the Cloud Computing Standardization landscape, in particular from the point of view of Users (e.g. SMEs, Administrations)*. The Phase 2 will conclude with a detailed report including the revised “snapshot” of the state of standards at the end of 2015.

Table 1: ETSI CSC identified standards

Description	Related Standards	Notes
Requirements specification	No related standards as yet	This is on-going work at TMF [2], OGF [3], OASIS [4], ODCA [5] SLA*[6], SLAware [7]. FP7 projects results [8]
Security & Privacy Requirements specification	<ul style="list-style-type: none"> No related Standards but there is some relevant information in Cloud Security Alliance’s “Security Guidance for Critical Areas of Focus in Cloud Computing” Cloud Security Alliance’s Cloud Control Matrix (CCM) V3.0 [12] ISO 27001/2 [13] 	<ul style="list-style-type: none"> There are a number of non-cloud computing-specific but widely used and very relevant security standards for example OAuth 2.0 [9], SAML 2.0 [10], Kerberos [11] CCM Contains answers about which security measures a provider has taken. If the provider is ISO 27001/2 certified, it shows a certain level of security measures are in place (which fulfils part of the Data Protection legislation).
Service assessment and comparison	<ul style="list-style-type: none"> WS-Agreement NIST 800-5r4 [14] ISO 27002 [15] ISO 27017 [16] 	WS-Agreement (Open Grid Forum GFD.192 [17]) is a recommendation for creating electronic SLAs



3 Adoption of standards within MUSA

Standards are important in the area of cloud computing for coherence and interoperability, and as such they are to be observed and adopted where pragmatic. In this section we consider the use of standards within the MUSA project and the potential impact they will have on the project.

The main goal of Standards analysis task within MUSA is to continuously observe the relevant standards around MUSA research topics and technologies in order to identify which should be adopted in the MUSA solution with the purpose of achieving a solution that can be easily adopted by the industry. If MUSA outcomes are relevant for the standardization bodies leading those standards, the consortium may contact them and promote those results with a Request for Proposal (RFP).

The detailed plan of standards adoption in the project is described in Section 3.5 below. Before, the Sections 3.1 to 3.6 describe the standards (together with the best practices that take the place of standards where no standards exist) relevant for MUSA main research areas (Section 3.1, 3.2, 3.3), other standardisation related initiatives that need to be watched closely (Section 3.4), and those standards and best practices that we initially intend to adopt (Section 3.5) and observe (Section 3.6).

The following table summarizes the existing, emerging and developing standards for initial consideration in MUSA, which are described in detail in Sections 3.1, 3.2 and 3.3 below.

Table 2: Summary of existing standards related to MUSA research topics

Standard	Owner	Comments
CloudML [18]	PaaSAGE [19], REMICS [20], ARTIST [21] MODAClouds [22]	Developed and expanded by the four projects, aligned with TOSCA. Although it is not a standard it is currently more developed than TOSCA and deserves inclusion at this stage of the project
TOSCA [23]	OASIS [4]	An emerging standard, likely to be influential in this space.
OCCI [24]	Open Grid Forum [3]	May influence on the interoperability of MUSA Security Assurance SaaS and the security mechanisms developed in MUSA.
CAMP [25]	OASIS	The monitoring mechanisms may be adopted in MUSA.
WS-Agreement [17]	Open Grid Forum	Was originally an IBM de-facto standard but became adopted by OGF.
SUoM [26]	Open Data Center Alliance	
NIST Cloud Reference Architecture (NIST 500-292 [27])	NIST	Cloud Computing Service Metrics Description [28] is part of NIST Cloud Computing Reference Architecture and Taxonomy Working Group
CSA MGW (not a standard)	Cloud Security Alliance [29]	A recently launched WG within CSA to deal with cloud metrics specification.



3.1 Standards for multi-cloud application modelling

3.1.1 CloudML

CloudML [18] is not currently the subject of a standards body working committee. As such it should not be included as a standard, however it has significance as it is already supported by four EU-funded research projects on Cloud (REMICS, PaaSAGE, ARTIST and MODAClouds). A thorough description of the utilisation of CloudML in the project will be made in WP2 *Multi-Cloud Security-by-design methods and tools*.

3.1.2 TOSCA

TOSCA [23] is a standardization technical committee under the aegis of OASIS. It is developing a standard specification to support the portability of cloud applications and services to provide a transparent interface for interoperability among the components. The goal of the TOSCA technical committee is to provide a standardised description of cloud services applications and infrastructures. The description is agnostic with respect of both vendor and technology. This would result in optimised and efficient usage of the cloud services. Portability in a vendor neutral eco-system is a cornerstone of TOSCA vision to allow dynamic, multi-cloud provider applications development without functional or non-functional compromises.

TOSCA Technical Committee (TC) is formed from members of many organizations actively participating in the development of the specification. The TOSCA TC is making progress in the development of the next major iteration of the TOSCA specification. The TOSCA TC has started work on the next release of TOSCA with the TOSCA Simple Profile for YAML. The next iteration is expected to be available as a Candidate OASIS Standard during the first half of calendar year 2015

TOSCA version 1.0 is now an OASIS standard. The use cases and examples considered in the current versions of TOSCA are developing and evolving. The new iterations of TOSCA will require more maturity in definitions and descriptions supported by the use cases. This will make it difficult for TOSCA to be adopted by MUSA. CloudML is aligned to TOSCA, and MUSA will keep a close observation of TOSCA.

3.1.3 OCCI

OCCI [24] standards for Open Cloud Computing Interface which is a set of open community-lead specifications delivered through the Open Grid Forum. Initially born as a remote management API for IaaS services, it has evolved into a REST based flexible API to solve interoperability, portability and integration issues in not only IaaS but also PaaS and SaaS service models too. The ultimate aim is to push towards fully open and interoperable clouds. As this is one of the interests of MUSA project too, the project will study the possibility of adopting OCCI in the development of the MUSA assurance platform in the form of a SaaS.

3.1.4 CAMP

The OASIS Cloud Application Management for Platforms (CAMP) [25] is a REST based interoperability protocol to package and deploy cloud applications, intended to be the first standardise Platform as a Service (PaaS) management API. CAMP defines interfaces for self-service provisioning, monitoring, and control, and it is expected to foster an ecosystem of common tools, plugins, libraries and frameworks, which will allow vendors to offer greater value-add.

In MUSA we will study the monitoring and control interfaces and tools of CAMP in order to decide whether they can be adopted as part of the monitoring mechanisms of the MUSA solution.



3.2 Standards for multi-cloud application security requirements specification in SLA

As stated in the Commission’s “Unleashing the Potential of Cloud Computing in Europe” Communication [48], cloud contract terms are often difficult to understand and mostly imposed, having the final consumer little power to negotiate or claim in the case the service has been discontinued or an incident has occurred. The accompanying staff working document [49] elaborates more on the need to have standardised Cloud contracts in order for final consumers and professional consumers to trust and uptake cloud computing: *Cloud provider contracts which disclaim liability, might contain unfair or illegal clauses and lack certain key pieces of information such as the location of data centres. In particular, service contracts offered to SMEs are rigid, with little room for negotiation. Stakeholders called for standardised contracts, with specific requirements regarding safety, security and reliability.*

In order to overcome these limitations, the EU is pushing a number of initiatives on the matter such as the Cloud Select Industry Group (C-SIG) on SLAs and the Code of Conduct (CoC) in DG Connect [50], the Expert Group on Cloud Computing Contracts in DG Justice [54], the European Cloud Partnership (ECP) [55], the Comparative Study on cloud computing contracts from DG Justice [56] and the study on Standards terms and performance criteria in service level agreements for cloud computing services from DG Connect [57]. Security accreditation will empower cloud service consumers.

3.2.1 WS Agreement

Web Services Agreement Specification (WS-Agreement) is a Web Services protocol for establishing agreement between two parties, such as between a service provider and consumer, using an extensible XML language for specifying the nature of the agreement, and agreement templates to facilitate discovery of compatible agreement parties. The specification consists of three parts, which may be used in a composable manner: a schema for specifying an agreement, a schema for specifying an agreement template, and a set of port types and operations for managing agreement life-cycle, including creation, expiration, and monitoring of agreement states [17].

WS-Agreement born in the context of GRID computing and it is the only standard supporting a formal representation of SLAs and a protocol that aims at their automation. The main limit of such solution is that it was devised in a well-defined technological context, and that it is not completely fit in other contexts, such as clouds. The majority of the cloud-oriented FP7 projects (Contrail [41], mOSAIC [42], Optimis [43], PaasSage [19], SPECS [40]) are inclined to adopt WS-Agreement representations, suitably adapted to the cloud context, as an example offering the WS-Agreement protocol using REST instead of Web Services like in [46] from Optimis Project.

WS-Agreement offers a schema to represent both *Templates* and *SLA Offers*, in order to enable simple negotiation processes among SLA Providers and Consumers.

A SLA Offer is the description of the agreement relationship that is sent from initiator¹ to responder² during agreement creation, indicating the relationship, which the initiator would like to form. This offer is accepted or rejected by the responder. In practice, they are the documents that will be signed by both parties that states the terms of the contract. It contains a description of the services covered by the SLA and a set of Guarantee Terms that states the grants over the services.

¹ *Initiator* is a party of an agreement that creates and manages an agreement on the availability of a service on behalf of either the service consumer or service provider, depending on the domain-specific requirements

² *Responder* is a party of an agreement that implements and exposes an agreement on behalf of either the service provider or service consumer, depending on the domain-specific requirements.



SLA Templates are documents used by the agreement responder to advertise the types of offers it is willing to accept. As an SLA Offer document, the template is composed of a name, a context element, and agreement terms, but additionally also includes information on agreement creation constraints to describe a range of agreements it might accept.

The XML Language proposed by WS-Agreement can be easily extended in order to represent domain specific Service Level objectives.

3.2.2 SUoM

SUoM [26] is a standard developed by the Open Data Center Alliance, which describes a set of standard service parameters for IaaS, in 4 different levels (Bronze, Silver, Gold, Platinum), and covers among other things, security, availability, and elasticity.

3.3 Standards for Cloud computing service metrics

3.3.1 NIST Cloud Reference Architecture (NIST 500-292)

From the days of service oriented architecture there has been a perceived need to be able to compare the functional and non-functional characteristics of services and this need has carried into the cloud services domain. Several initiatives were started to solve this problem and an extension was developed to W3C's Web Services Description Language to enable semantic annotations. This attempt was superseded by the Service Measurement Index (SMI), measuring the "relative goodness" of services. SMI was part of the early discussions at NIST for forming a standard based on the description of metrics that can describe a cloud computing service [28]. This is seen as an extension to the NIST Cloud Computing Reference Architecture.

NIST has published the guide on metrics in January 2015 and this guide will be used as part of the guide to the way that cloud services are described within this project.

3.3.2 ISO Cloud SLA framework (ISO/IEC NP 19086)

The ISO organisation is also working in metrics and requirements for SLAs together with metrics and controls to be applied. The working standard is the ISO/IEC NP 19086 *Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology* [52] which includes:

- ISO/IEC NP 19086-1 - Part 1: Overview and concepts
- ISO/IEC NP 19086-2 - Part 2: Metrics
- ISO/IEC NP 19086-3- Part 3: Core requirements

3.3.3 CSA

The Cloud Security Alliance has recently formed a working group (MWG) active in the area of security metrics that may complement or influence NIST. MUSA will observe the progress of this working group as well as the SPECS [40] project's work in this area.

3.4 Related organisations and initiatives

3.4.1 EC CSIG

The Cloud Select Industry Group [50] is a group of industry stakeholders advising the European Commission on cloud computing policy actions. Particularly, the subgroup on service level agreements helps the Commission to develop model terms for Cloud computing SLAs.

Their work has led to the publication of the *Cloud Service Level Agreement Standardisation Guidelines* [51] which describe the service level objectives of the cloud services that may be included in cloud SLAs. These SLOs are classified in four big areas: performance, security, data management and personal data protection. The guidelines will further contribute to the ISO/IEC 19086 project [52].



3.4.2 CSA

Cloud Security Alliance is leading private organisation that has a mission to promote the use of best practices for cloud computing security. There are 25 working groups looking into cloud standards, certification, education and training. Some of the initiatives that are worthy of further examination are the CSA Governance, Risk and Compliance stack (GRC) that delivers a toolkit for assessing both private and public clouds against industry established security best practices. The GRC includes the following initiatives:

- **CloudAudit:** a common interface and namespace to allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their cloud services.
- **Cloud Controls Matrix (CCM):** a controls framework that collects security measures or controls implemented in cloud services. The CCM includes the mapping of the controls to those of other industry-accepted security standards, regulations, and controls frameworks.
- **Consensus Assessments Initiative Questionnaire (CAIQ):** a questionnaire for cloud providers to document what security controls do they apply, aimed at their transparency.
- **Cloud Trust Protocol (CTP):** a protocol for cloud service consumers ask for and receive information form cloud providers about compliance, security, privacy, integrity, and operational security of the cloud service.

CSA is particularly active, for example they recently published a whitepaper entitled *Best Practices for Mitigating Risks in Virtualized Environments* [30] that gives guidance on identification and management of risks in a virtualised environment. Many of the practices are indicated by ENISA as noted in Table 3.

3.4.3 CSCC

Cloud Standards Customer Council [31] is an end user association that works on promoting and easing the adoption of Cloud technologies. The work includes contributions in the areas of standards, security and interoperability.

Their works on cloud security and SLAs are those that are of main importance for MUSA, such as *Security for Cloud Computing: 10 Steps to Ensure Success V2.0* [32], *Cloud Security Standards: What to Expect & Negotiate and Practical Guide to Cloud Service Agreements V2.0* [33].

3.4.4 MPAA

The significance of the Motion Picture Association of America is based on their work in the area of content security. Theft or piracy of films is a major concern and has led to a series of best practices that define both physical and digital security for content. These practices are not all applicable in a cloud computing environment, for example the I/O Device security may not seem to be applicable in a cloud environment but there are a number of areas where these best practices are of importance. The best practices are freely available on the website [34] and have been updated in 2013. It is interesting to note that the best practices go well beyond the requirements of Cloud Computing to develop security practices relating to transport, shipping and budgeting.

3.4.5 ENISA guidelines on cloud security









There are a number of works on cloud security issued by the European Network and Information Security Agency. The most relevant for MUSA can be summarized as follows:

- **Security service level monitoring:** Cloud computing brings new challenges for IT personnel whose role is focussed on the proper establishment and monitoring of cloud controls with the IT providers. ENISA security service level monitoring helps with the optimisation of information security as part of the contracts that enforce SLAs.





















- **Procure Secure** [35]: This is a guideline that supports IT procurement teams in how to monitor and control the security parameters of cloud services. The guide classifies the security parameters covered into eight major types: service availability; incident response; service elasticity and load tolerance; data lifecycle management; technical compliance and vulnerability management; change management; data isolation; and log management and forensics. Besides describing each of the parameters and providing examples to clarify their meaning, the guide concludes with a checklist to aid in the continuous control of such security parameters on the procured services.
- Following this line of work, ENISA has recently released in April 2015 their Cloud Security Guide for SMEs [36], which includes the most important eleven (11) security risks and eleven (11) security opportunities for SMEs to take into account when procuring a cloud service. The guide includes a list of twelve (12) targeted security questions the SME could pose to the provider to understand the level of security of the service. The guide is accompanied by a tool [37] to support the rating of the risks and opportunities according to the SME's requirements and the generation of the customised list of security questions to collect information on the security measures adopted by the cloud provider for a particular service.
- There also exist other related previous ENISA works such as the *Security and Resilience in Governmental Clouds* [58], and the *Cloud Computing Security Risk Assessment Rev. B* [60] and the *Survey on security parameters in cloud SLAs* [61] that already paved the path towards awareness on the need of more comprehensive SLAs for better control of provided features and security and privacy risks.
- With the aim of further facilitate the procurement of cloud services while taking into account the security, ENISA is also working in Cloud Certification [38] schemes clarification: In the last months ENISA is also working in the clarification of the current cloud certification landscape. Their work is mainly addressing two parts:
 - a) The Cloud Certification Schemes List (CCSL): a collection of different existing certification schemes.

Table 3: Cloud Certification Schemes List

Certification scheme logo	Organisation	Certification scheme
	TÜV Rheinland 	Certified Cloud Service – TÜV Rheinland
	Cloud Security Alliance (CSA) 	CSA Attestation – OCF Level 2
	Cloud Security Alliance (CSA) 	CSA Certification – OCF Level 2
	Cloud Security Alliance (CSA) 	CSA Self Assessment – OCF Level 1



	EuroCloud 	EuroCloud Self Assessment
	EuroCloud 	EuroCloud Star Audit Certification
	ISO 	ISO/IEC 27001 Certification
	PCI Security Standards Council 	Payment Card Industry Data Security Standard v3
	Leet Security 	Leet Security Rating Guide
	American Institute of Certified Public Accountants (AICPA) 	Service Organization Control (SOC) 1
	American Institute of Certified Public Accountants (AICPA) 	Service Organization Control (SOC) 2
	American Institute of Certified Public Accountants (AICPA) 	Service Organization Control (SOC) 3
	Cloud Industry Forum 	Cloud Industry Forum Code of Practice

- b) The Cloud Certification Schemes Metaframework (CCSM) which is a meta-framework or high level mapping from the customer's Network and Information Security requirements to security objectives in existing cloud certification schemes. The CCSM includes a supporting online tool that generates a matrix which maps desired security objectives of the cloud service to different cloud certification schemes, and it generates procurement checklists or questionnaires to aid the customers in cloud procurement.

3.4.6 CloudWatch works on cloud security

Other relevant work on clarifications on Cloud certifications and standardisation are the ones accomplished by CloudWatch Hub EU CSA project, named *Cloud certification guidelines and recommendations* [65].



As part of its mission to making an active contribution to cloud standards, CloudWatch has issued a collection of *Guidelines on how to protect personal data in cloud service contracts* that compiles a set of legal tips and recommendations for contractual clauses to which cloud consumers should pay attention when contracting cloud services in order to ensure personal data is appropriately protected.

The standards for cloud security identified in the *Best practices for Cloud standards profile development guide* by CloudWatch are:

- ISO / IEC 27018 Code of practice for data protection controls for public cloud computing services
- NIST 800 – 53 Rev.4 Security Controls
- NIST Security Reference Architecture
- Cloud Controls Matrix (CCM), Cloud Security Alliance
- Open Certification Framework (OCF), Cloud Security Alliance
- Cloud Trust Protocol (CTP), Cloud Security Alliance
- CloudAudit, Cloud Security Alliance
- Privacy Level Agreement, Cloud Security Alliance
- Star Audit, Euro Cloud
- Data Security Framework, Open Data Center Alliance

In addition, the standards for cloud SLAs identified by CloudWatch are:

- Web Services Agreement (WS-Agreement) – OGF
- A WS-Agreement Based SLA Implementation for the CMAC Platform
- WS-Agreement Negotiation – OGF
- SLA: An abstract syntax for Service Level Agreements – SLA@SOI
- GB917 SLA Management Handbook, Release 3.1 –TM Forum
- TR178 Enabling End-to-End Cloud SLA Management, Version 0.4 –TM Forum

CloudWatch is also currently working in the definition of *profiles for cloud standards* with the aim of reducing ambiguity in standards and achieve real interoperability across different interfaces. A standard profile serves to clarify how a standard has to be interpreted in a specific use case in order to ease its implementation in such use case. As a starting point for this, CloudWatch has developed a portfolio of European and international use cases on technical, policy and legal requirements. The ultimate goal is to derive common standards profiles from these use cases and test them around a federation of cloud services.

3.5 Standards and best practices planned for adoption in MUSA

At the time of publication of the present document, a set of standards area set of standards is planned for potential adoption in MUSA. This initial set will grow as the project research progresses and technical decisions are made. The list of standards identified for adoption will be maintained in the Standardisation observatory task in MUSA for discussion and further work. Therefore, this section of the report will develop further over the coming periods of the project.

The overall view of the initial list is shown below in Table 4. The table indicates the name of the standard or best practice, the body that is responsible for the specification, the status of the standard (adopted, observed, not applicable in MUSA) and which Work Package in MUSA carries out the research that will adopt or observe such standard. As said, this information may change over time. Thus, the table includes some clarifying notes for freeform to add comments or explanation of updates.



Table 4: Initial list of standards and best practices for adoption

Standard/Best practice	Standards Body	Status	Work Package	Notes
ISO 17789	ISO	Published	WP1	Definition of main roles in cloud architectures and basis for MUSA process roles.
ETSI TR 103 125 V1.1.1 (2012-11) technical report [66]	ETSI	Published	WP2	Definition of main roles in cloud SLA and recommendations for SLA specification.
WS-Agreement	OGF	Published	WP2	Language for cloud SLAs specification.
NIST Cloud Reference Architecture (NIST 500-292)	NIST	Published	WP3	Considered as the basis for the cloud services metrics description.

3.6 Additional standards under observation

There are a number of additional standards and best practices that need to be included under the surveillance of MUSA for completeness. These standards will form part of the Observatory list of standards. Most of them have been already identified and explained in previous sections.

Table 5: Other standards under observation of MUSA

Standard	Standards Body	Relevance to MUSA
Cloud		
ISO NP 19086 Service Level Agreement (SLA) Framework and Terminology	ISO/IEC	Cloud SLA with security properties - WP2
ISO Cloud Reference Architecture (ISO 17788 and 17789)	ISO/IEC	General reference for cloud architecture, processes, use cases and actors/roles – WP1
ETSI Cloud Standard Coordination reports	ETSI CSC	General reference for cloud standards.
CSCC Practical Guide to SLA	CSCC	Cloud SLA with security properties - WP2
CSCC Cloud Use Cases	CSCC	General reference for cloud architecture, processes, use cases and actors/roles – WP1
CSCC Cloud Use Cases – Moving to the Cloud	CSCC	General reference for cloud architecture, processes, use cases and actors/roles – WP1
Security		
NIST Control Framework 800-53r4	NIST	Security controls and metrics
ISO 27001	ISO/IEC	Management system framework for



		information security.
ISO 27002	ISO/IEC	Security controls.
ISO 27017	ISO/IEC	Cloud security controls.
GRC (includes CCM)	CSA	Cloud security controls, metrics, and trust protocols.
CSCC Security for Cloud Computing	CSCC	Cloud security controls, metrics, certifications and best practices.
ENISA guidelines on NIS and resilience.	ENISA	Cloud security controls, metrics, certifications and best practices.

The MUSA solution will be prototyped and deployed in AIMES partner who adopts international standards such as the Data Centre Alliance Accreditation (DCA), ISO27001 and EuCOC [39]. AIMES also adhere to regional accreditations such as NHS Information Governance.

3.7 Plan for Adoption of Standards in MUSA framework

The standards adoption plan that has been defined in MUSA includes concrete strategic actions, as follows:

1. Identification phase (already finished): We have worked in analysing the standards relevant for each of the parts of the MUSA solution. This document collects the results of this initial phase.
2. Continuous observatory: the cloud standards landscape will be continuously monitored by the partners responsible of standardisation in MUSA who will check for new initiatives related to the research work being done in the project. This work will be carried out within the Standards Observatory named task in MUSA.
3. Integration in MUSA components: Both WP2 and WP3 will adopt the corresponding standards in their own developments, WP2 – sections 3.1 and 3.2, WP3 – section 3.3. No standards exist for WP4 monitoring, but we try to follow best practices identified in previous section as much as possible.
WP1 has defined the requirements of MUSA solution and the adopted standards will need to support them.
Finally, in WP1 we will also develop the MUSA guide for multi-cloud application security-intelligent lifecycle management promoting DevOps and security-by-design best practices.
4. Liaison with identified standardisation bodies: The work in MUSA may lead to the need of proposing extensions or modifications to the adopted standards. In those cases, the consortium will evaluate the work to be done, and define a responsible partner for keeping the contact with those standardisation bodies responsible for the standards subject to this work. This will serve for better knowing the next steps towards the inclusion of MUSA contributions in the standards.
5. Pushing of new standards: Depending on the relevancy of the obtained results and the result of the analysis of the needed work for the standards extension, the consortium will evaluate the possibility of pushing MUSA results as (additions to) standards.
6. Standardisation plan review: This plan will be revised in one year time with the results of the actions included in the plan and the possible additional standards that may have rose as relevant for MUSA in this period.
The last revision of the plan will be made at the end of the project, when we will report the results of the standardisation plan, including adopted and contributed standards (if any).

We anticipate that the first three strategic steps above, i.e. identification, observation and integration in MUSA components, will ask for a series of activities that will be continuous. These are illustrated in



Figure 1. It should be noted that the first box in Figure 1 is a continual process referred to as the cloud Standards Observatory. The observatory reviews new and emerging standards and evaluates them for adoption by the project on a regular basis.

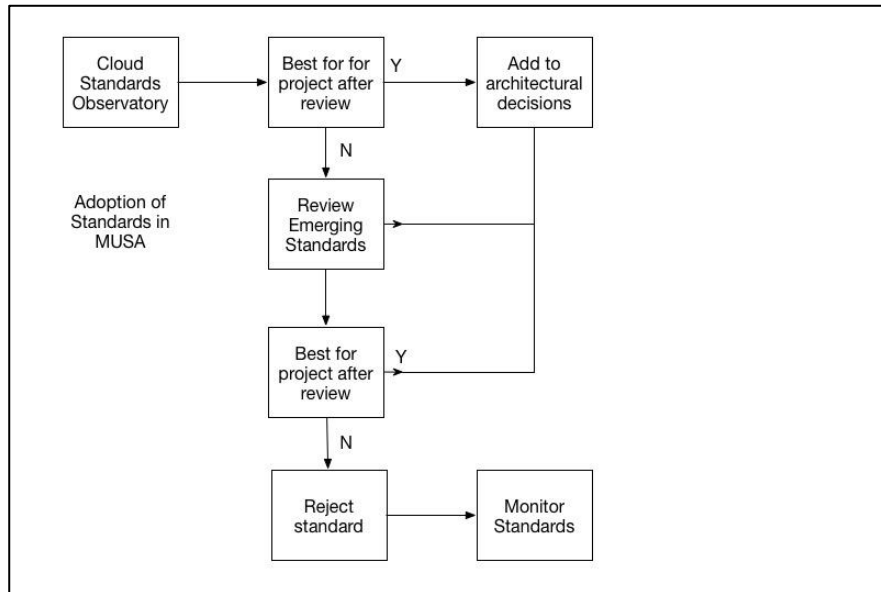


Figure 1: Plan for adoption of standards

4 Impact of MUSA on standards

4.1 The role of the consortium in developing and emerging standards

Standards are the lifeblood of integration and interaction in IT. Without standards from a number of bodies there would be a disparate group of technologies that require different links or connectors to be written for each one. There are two types of standards, the De-Facto standards, standards that are adopted by IT because they seem a good fit for the purpose. These are not enforced by standards bodies and certification but by general agreement. There is one major problem with this style of standard and that is the continued support by one or two organisations that manage the standard. De-Jure standards are those that are agreed with a standardisation body, managed and maintained with mutual agreement and support from the community and not just the dominant technology providers in that domain. The problem with De-Jure standards is the length of time that they take to produce a certified specification and recommendation. In both types of standard the community is vital glue that holds the standard together.

Influencing a standard is difficult unless it is done at an early stage in its development. Indeed the recognised way of promoting a standard to a standards body and creating a technical committee is to form a community around a tentative standard technology and once the tentative standard is in good shape propose this to the standardisation body as a package with specification, objectives and a community in place. This is exemplified by the contrast between CloudML (a de-facto standard) and TOSCA (a de-jure standard) both covering similar areas with CloudML being developed and promoted through a number of EU-funded research projects, PaaSage, REMICS, ARTIST and MODAClouds and TOSCA being supported by OASIS. In this circumstance the potential conflict is resolved by aligning CloudML with TOSCA and registering CloudML as a TOSCA aligned project. This solution, however, may take longer than the lifetime of MUSA project.

The timeframe and logistics for developing a new standard specification are sufficiently complex and lengthy that it is unlikely that any standard specification will result directly from work in MUSA. The time frame is often measured in 2 or 3 years. It can be seen that the project will have little chance to develop a new standard, however there are a number of emerging standards that may benefit from work by the consortium. Benefits to emerging standards depend on the involvement and commitment of consortium partners. Benefits may be difficult to realise in the more mature draft specifications because there is little room for change and extension in mature specifications..

4.2 Influence on standards

MUSA will still have an impact on standards due to the involvement of members of the consortium. TECNALIA is a contributor to ISO IT security techniques (ISO/IEC JTC 1/SC 27) and cloud reference architecture (within ISO/IEC JTC 1/SC 38), for example, and CA Technologies is a contributor to TOSCA, NIST, OASIS and W3C. These contributions will benefit from the partners membership of the MUSA consortium and indirectly influence the relevant standards.



5 Conclusions

There are a wide variety of standards and best practices ranging from the International Organisation for Standardisation to the EU-funded research projects. These all have a potential impact on the MUSA project. This document has outlined the relevant standards and best practices and described the strategy for ensuring that the project adheres to them where practical. Taking an idea and draft standard specification through to becoming a recommendation often takes a long time. For this reason the project is unlikely to initiate a new standard and see it through to becoming a recommendation over the duration of the project. Work in the project can become influential with several members of the project partners participating on standards working groups or technical committees.

As part of this strategy the project has set up a standards observatory responsible for the continuous watch of the status and progress of the standards. On a periodic basis the standards observatory will review the standards and best practices for adoption and where necessary update the list of candidate standards for adoption and observation. The observatory will keep a central repository for this information.



References

- [1] ETSI Cloud Standards Coordination (CSC). Available at: <http://csc.etsi.org/>
- [2] TMF, TM Forum, Available at: <https://www.tmforum.org>
- [3] OGF, Open Grid Forum Available at: <https://www.ogf.org/ogf/doku.php>
- [4] OASIS Standards Organisation, Available at: <https://www.oasis-open.org>
- [5] ODCA Open Data Center Alliance, Available at: <http://www.opendatacenteralliance.org>
- [6] SLA* SAL@SOI SLA Infrastructure (FP7 Project) Available at: <https://www.tmforum.org>
- [7] SLAware – FI-Ware Available at:
https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Mapping_Cloud_Hosting
- [8] FP7 project results Available at:
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2496
- [9] OAuth 2.0 Next evolution of the OAuth protocol Available at: <http://oauth.net/2/>
- [10] SAML 2.0 Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- [11] Kerberos: Available at: <http://www.kerberos.org>
- [12] Cloud Security Alliance’s CCM V3.0 Available at:
<https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/>
- [13] ISO 27001/2 standard. Available at: <http://www.27000.org>
- [14] NIST 800-5r4 Available at: <http://csrc.nist.gov/publications/PubsFL.html>
- [15] ISO 27002 standard. Available at: <http://www.27000.org>
- [16] ISO 27017 standard. Available at: <http://www.iso27001security.com/html/27017.html>
- [17] WS-Agreement GFD.192 Available at:
<https://www.yumpu.com/en/document/view/21403326/gfd192-open-grid-forum>
- [18] CLOUDML. Available at: <http://cloudml.org>
- [19] PaaSage EU project. Model Based Cloud Platform Upperware. FP7- ICT-2011.1.2. 2012-2016. www.paasage.eu/
- [20] REMICS EU project, Available at: <http://www.remics.eu>
- [21] ARTIST EU project. Advanced software-based service provisioning and migration of legacy software. FP7- ICT-2011.1.2, 2012-2015. www.artist-project.eu/
- [22] MODAClouds project - Model-Driven Approach for design and execution of applications on multiple Clouds. FP7- ICT-2011.1.2. 2012-2015.
www.modacLOUDS.eu/project/
- [23] OASIS TOSCA standard v1.0 , Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
- [24] Open Grid Forum’s OCCI. Available at: <http://occi-wg.org>
- [25] OASIS CAMP standard. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp
- [26] SUoM. Available at: <http://www.opendatacenteralliance.org/accelerating-adoption/webcasts-and-videos>



- [27] NIST Cloud Reference, Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505
- [28] NIST Cloud computing service metrics description. Available at: <http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf>
- [29] CSA Cloud Security Alliance. Available at <https://cloudsecurityalliance.org>
- [30] CSA Best Practices for Mitigating Risks in a Virtualised Environment. Available at <https://cloudsecurityalliance.org/media/news/csa-launches-best-practices-for-mitigating-risks-in-virtualized-environments/>
- [31] CSCC. Available at: <http://www.cloud-council.org>
- [32] Security for Cloud Computing. Available at <http://cloud-council.org/resource-hub.htm/>
- [33] Cloud Security Standards. Available at: <http://cloud-council.org/resource-hub.htm/>
- [34] MPAA best practices. Available at <http://www.fightfilmtheft.org/best-practice.html>
- [35] ENISA Procure Secure. Available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts>
- [36] Cloud Security Guide for SMEs <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes>
- [37] SME Guide Tool: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/sme-guide-tool>
- [38] ENISA Cloud Computing Certification. Available at: <https://resilience.enisa.europa.eu/cloud-computing-certification>
- [39] EuCOC. Available at: http://www.data-central.org/?page=EUCoC_EE
- [40] SPECS Project. Secure Provisioning of Cloud Services based on SLA management. FP7- ICT-2013.1.5, 2013-2016. <http://specs-project.eu/>
- [41] CONTRAIL EU project. Available at: <http://www.juniper.net/us/en/products-services/sdn/contrail/>
- [42] mOSAIC Open-Source API and Platform for Multiple Clouds EU project. Available at: <http://www.mosaic-cloud.eu/>
- [43] OPTIMIS EU project. Available at: <http://www.optimis-project.eu/>
- [44] ENISA, Cloud Standards and Security. Available at: <https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf>
- [45] ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms standards catalogue. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=601355
- [46] R. Kubert, G. Katsaros, and T. Wang, “A RESTful implementation of the WS-Agreement specification,” in Proceedings of the Second International Workshop on RESTful Design, ser. WS-REST ’11. New York, NY, USA: ACM, 2011, pp. 67–72.
- [47] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, and M. Xu, “Web services agreement specification (WS-Agreement),” in Global Grid Forum. The Global Grid Forum (GGF), 2004



- [48] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (2012), “Unleashing the Potential of Cloud Computing in Europe”. Available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.
- [49] Commission Staff Working Document accompanying the document Unleashing the Potential of Cloud Computing (Brussels, 27.9.2012 SWD(2012) 271 final). Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012SC0271>
- [50] Cloud Select Industry Group - Digital Agenda for Europe - European Commission. Available at: <http://ec.europa.eu/digital-agenda/en/news/cloud-select-industry-group>.
- [51] Cloud Service Level Agreement Standardisation Guidelines. Available at: <http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>
- [52] ISO/IEC 19086 project. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902
- [53] CSA’s GRC stack. Available at: https://cloudsecurityalliance.org/research/grc-stack/#_overview
- [54] Expert Group on Cloud Computing Contracts (E02922) in DG Justice. Available at: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2922>
- [55] The European Cloud Partnership (ECP). Available at: <http://ec.europa.eu/digital-agenda/en/european-cloud-partnership>.
- [56] EC DG Justice Open call for tender: Comparative Study on cloud computing contracts –JUST/2012/EVAL/PR/0116/A4. Available at: http://ec.europa.eu/justice/newsroom/contracts/files/2013s084-140907/invitation_en.pdf.
- [57] EC DG Connect Call for tenders: Study on standards terms and performance criteria in service level agreements for cloud computing services - SMART 2013/0039. Available at: <http://ec.europa.eu/digital-agenda/en/news/call-tenders-study-standards-terms-and-performance-criteria-service-level-agreements-cloud>.
- [58] Security and Resilience in Governmental Clouds. ENISA January 2011. Available at: <http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds>
- [59] Procure Secure: A guide to monitoring of security service levels in cloud contracts. ENISA April 2012. Available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts>
- [60] Cloud Computing Benefits, risks and recommendations for information security. Rev B December 2012. Available at: <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security>
- [61] Survey and analysis of security parameters in cloud SLAs across the European public sector. ENISA December 2011. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector>



- [62] Cloud Computing Service Level Agreements-Exploitation of Research Results. European Commission, June 2013. Available at:http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2496. .
- [63] ETSI CSC Final Report Cloud Standards Coordination Final Report, November 2013, v 1.0. Available at:
<http://csc.etsi.org/Application/documentApp/documentinfo/?documentId=204&fromList=Y> .
- [64] CSCC-Public Cloud Service Agreements: What to Expect and What to Negotiate. Available at: <http://www.cloud-council.org/publiccloudSLA.pdf> .
- [65] CloudWATCH Cloud Certification on Guidelines and Recommendations. Available at:
http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Cloud_certification_guidelines_and_recommendations_0.pdf
- [66] ETSI TR 103 125 v1.1.1 (2012-11). Available at:
http://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf
- [67] MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017. Available at:
www.musa-project.eu



Appendix A. MUSA motivation and background

The main goal of MUSA project³ 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.

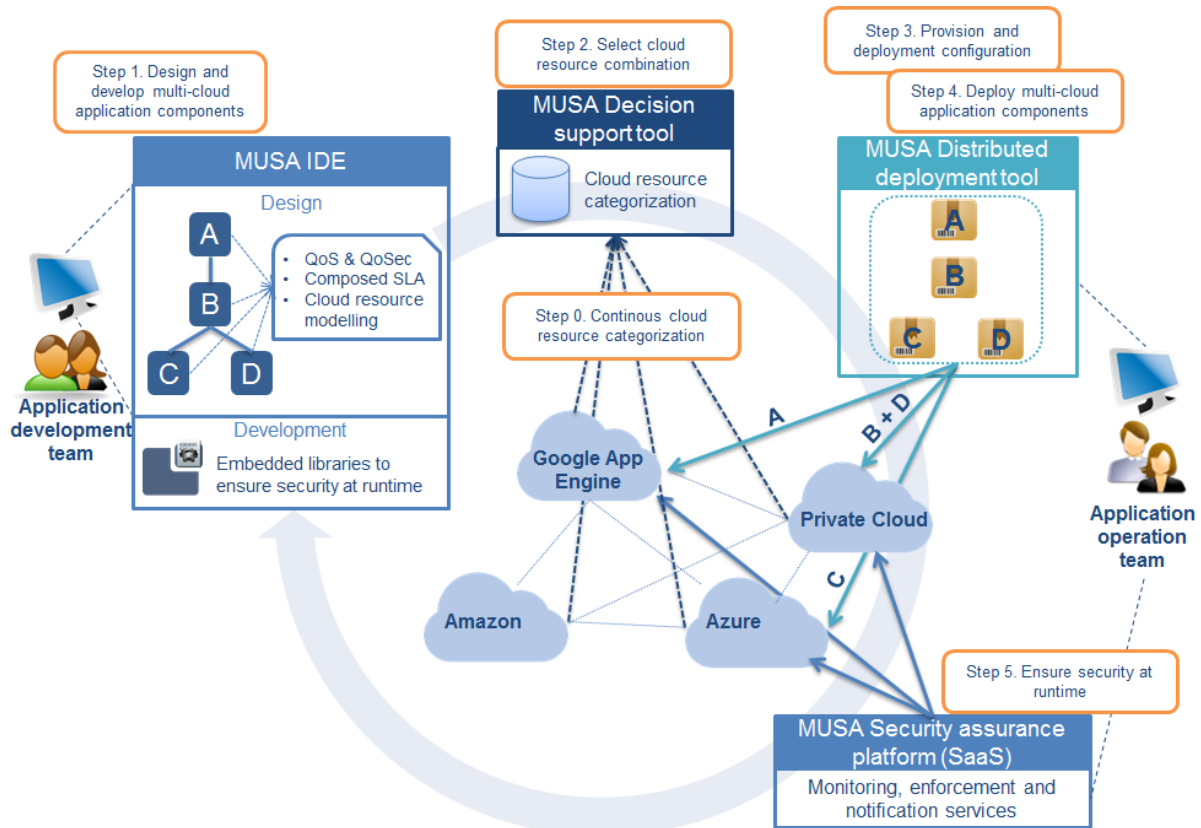


Figure: MUSA overall concept

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.

³ MUSA H2020 Project, Multi-cloud Secure Applications. 2015-2017, <http://www.musa-project.eu>