MUlti-cloud Secure Applications

Deliverable title	Deliverable ID: D7.7
	Preparation date: 22/12/2017
Standards Adoption Report	Editor/Lead beneficiary (name/partner): Peter Matthews / CA
	Internally reviewed by (name/partner): Antony Shimmin / AIMES Valentina Casola / CERICT

Abstract:

This is the final report of the standards observatory for the MUSA project. It builds on work in D7.5 and D7.6 to give a final view of standards that have been observed in addition to standards that have been adopted. It may need to be read in conjunction with both those deliverables since some standards have not changed and are merely referred to in this document whilst others have moved considerably. Many of the entries in this document describe deltas from previous standards deliverables. Standards are continually evolving and being created. This is not an exhaustive analysis, but an analysis of standards that have a relationship with application composition from cloud services, secure cloud services and agile methodologies.

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 Muntes 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 (LHS, Germany)	Contact: Dirk Bracklow dirk.bracklow@lhsystems.com
	TTY-säätiö (TUT, Finland)	Contact: José Luis Martínez Lastra jose.lastra@tut.fi

Table of contents

List of tables

Executive summary

This is the final report of the Standards Observatory in the MUSA project. It builds on work reported in D7.5 and D7.6 and delivers the current status of standards as either full updates where there are many changes and developments or as deltas where there is little movement. Full updates are provided for standards such as TOSCA and a delta for a standard that has little changed, such as Motion Picture Association of America (MPPA). Many of the standards mentioned are still in development that may or may not remove them from any MUSA development. There are three main sections that cover the information regarding the standards being followed as part of the observatory, the standards and best practices being adopted and finally the standards that are under observation and their relevance to MUSA.

Many of the standards that are applicable to the MUSA project have changed little. It is, sadly, a feature of de-jure standards that working groups often take a considerable time to reach a recommendation. Some more foundational de-jure standards are strongly supported and driven at a fast pace. These standards are generally more applicable than the less well supported standard. As mentioned earlier TOSCA is a foundational standard that receives a great deal of attention, there is an extensive view of TOSCA in this final report and it is interesting to note the synergy between TOSCA, multi-cloud modelling, covered in the CloudML section, the MUSA Decision Support Tool, the MUSA Modeller and the MUSA Deployer. Many of the standards bodies develop similar or even overlapping standards.

In a departure from previous reports two significant methods of managing threats and risk have been included because of their significance to MUSA. STRIDE and ROAM are not standards in the context of being under the management of a standards body, but they are accepted by agile developers and the risk and security management community as best practices and could justifiably be regarded as de-facto standards. These are contained in the section on standards and best practices adopted in MUSA.

The report continues with a table of relevant standards that are under observation indicating the relevance to MUSA.

In conclusion, the report notes that there is still on-going work in all areas of standards with a few exceptions. Security is pervasive in all applications and environments and there are many standards that touch or are entirely dedicated to security. This report is not exhaustive, but covers the most appropriate standards and best practices for the MUSA project

1 Introduction

1.1 Ojective of this document

This document is deliverable D7.7 *Standards adoption report* of the MUSA project [1].

The main objective of this document is to describe the final collection of standards and best practices adopted in MUSA project. The Standards Observatory task in the project served to keep track of the progress in cloud standards and to identify which ones were more relevant for MUSA and which ones could be adopted in the different mechanisms and tools in the MUSA framework.

1.2 Structure of this document

The document is structured as follows. After this introductory section, Section 2 provides a final review of the progress in standards covered under the Standards Observatory. Then, Section 3 reports the standards adopted within MUSA project. Section 4 collects relevant standards related to security assurance in multi-cloud applications. Finally, Section 5 concludes the document. The Appendix A summarizes the MUSA project motivation and background.

1.3 Relationships with other deliverables

The present deliverable D7.7 and the standards details presented in this document relate to the following deliverables of the project:

- *D7.5 Standards analysis and strategy plan*, M6: This deliverable presented the initial version of standards strategy plan of MUSA project that was revised and completed in the D7.6.
- *D7.6 Revised Standards Strategy Plan*, M18: This deliverable presented the revised version of standards strategy plan of MUSA project that included a revised standard analysis and adoption plan.

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	Cloud Control Matrix	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
OCCI	Open Cloud Computing Interface		

1.6 Revision history

Version	Date issued	Author	Organisation	Description
1.0	3/06/2017	Peter Matthews	CA	Initial Table of contents for agreement
1.1	2/07/2017	Peter Matthews	CA	Agreed Table of contents and initial contributors
1.2	5/09/2017	Peter Matthews	CA	Updated CA Contributions
1.3	24/10/2017	Erkuden Rios	Tecnalia	Agreed updates and data
1.4	8/11/2017	Erkuden Rios	Tecnalia	Additional data and final action plan
1.5	30/11/2017	Max Rak	CERICT	NIST and other standards update
1.6	4/12/2017	Peter Matthews	CA	Merge in changes, exec overview and conclusions
1.7	4/12/2017	Erkuden Rios	Tecnalia	Completed and formatted.
1.8	5/12/2017	Peter Matthews	CA	Final Review draft
1.8.1	13/12/2017	Valentina Casola	CERICT	Final Review CERICT
1.8.2	13/12/2017	Antony Shimmin	AIMES	Final Review AIMES
1.9	19/12/2017	Peter Matthews	CA	Final Revised
2.1	22/12/2017	Erkuden Rios	Tecnalia	Final Release.

2 Standards progress

This section will describe changes to standards that have been monitored since D7.6 delivered in M18.

2.1 Standards for multi-cloud application modelling

2.1.1 TOSCA

TOSCA is a standardization technical committee under the aegis of OASIS. The committee has developed an open standard to facilitate the deployment, orchestration and management of cloud applications and services across the entire lifecycle of the application. The TOSCA standard uses a domain-specific language (DSL) to describe, in a portable format, cloud applications, services, platforms, infrastructure and data components, along with their relationships, requirements, capabilities, configurations and operational policies. The description is agnostic with respect to both vendor and technology. These descriptions facilitate portability and automated management across cloud providers regardless of underlying platform or infrastructure. Portability in a vendor neutral eco-system is a cornerstone of the TOSCA vision to support dynamic, multi-cloud provider application development.

The TOSCA Technical Committee (TC) one of the largest in the history of OASIS, and is composed of members from numerous multi-national companies and universities and has liaisons with major international standards organizations including ISO/IEC JTC 1 SC38 [2], ETSI NFV [3] and EU FP7 projects.

The first version of the TOSCA specifications was released in November 2013 called: Topology and Orchestration Specification for Cloud Applications Version 1.0 [4]. A subsequent version of the standard called TOSCA Simple Profile in YAML v1.0 was released in January 2017 that leveraged feedback from multiple TOSCA implementers, including those from open source communities, e.g., OpenStack, Apache, Eclipse, etc., to offer real-world, use case driven refinements to TOSCA, while also better aligning with popular tools and platforms in the open source community through a less verbose and more human-readable YAML rendering.

The TOSCA Simple Profile in YAML v1.1, which features the addition of fully declarative workflow enables TOSCA orchestrators to take actions based on declarative operational policy, has finished its 2nd public review in March 2017, and could reasonably be expected to become an OASIS standard before the end of 2017.

Driven by the rapidly evolving ETSI NFV standardization and open source communities, the TOSCA Simple Profile for NFV is currently under development in parallel with the TOSCA Simple Profile in YAML v1.2. Together they will support the NFV use cases and examples.

This version will also add much richer and more flexible support for artefact processors, making the essentially “first-class” entities in TOSCA Service Templates and describing how TOSCA orchestrators will work with them when encountering Artefacts within a Topology. The intent is to include several examples showing how well-known Artefact types would be processed, e.g., Bash and Python (scripts) types, traditional Virtual Machines (VMs), or container images. TOSCA orchestrator integration with advanced workflow languages, e.g., BPEL and BPMN, as new Artefact types will also be covered.

There is also work being done in parallel on a TOSCA Instance Model that will enable the representation of the current state of a TOSCA deployment including all inputs, concrete node fulfilments, property settings, cardinalities, relationships, applied policies, and correlation with external resources and entities.

Considering the very rapid evolution of the TOSCA standard, it may be a challenge for MUSA to adapt to all the new possibilities and use cases presented. A similar challenge may present itself to

other communities interested in TOSCA. CloudML efforts are on a path of aligning it to TOSCA, and MUSA will continue to monitor and engage with the TOSCA community.

2.1.2 CloudML

CloudML language [5] 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 (PaaSage [6], REMICS [7], ARTIST [8] and MODAClouds [9]). A thorough description of the utilisation of CloudML in the project is included in deliverable D2.4 *Final MUSA IDE for security-aware design of multi-cloud applications*. In fact, the CloudML version that MUSA has adopted is the one of PaaSage project because it is the one included in the CAMEL language developed in PaaSage [10], which was adopted and extended in MUSA for multi-cloud application modelling [11].

2.1.3 OCCI

In the interval between D7.6 and this deliverable the Open Cloud Computing Interface has been published as a recommendation. There have been no changes between October 2016 and the time of publishing D7.7. The Open Grid Forum has published the recommendation as GFD 221-224 and GFD 226-229 [12].

2.1.4 CAMP

The OASIS Cloud Application Management for Platforms (CAMP) [13] 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.

2.2 Standards and best practices for multi-cloud application security requirements specification in SLAs

2.2.1 WS-Agreement

WS-Agreement standard [14] has not changed in the latest period. The MUSA Security Service Level Agreement (SLA) machine-readable format relies on the latest version of WS-Agreement, adopting the security extensions proposed by SPECS project [15]. The security SLA is the basis for SLA specification in MUSA SLA Generator tool.

2.2.2 SLALOM SLA

The project ended on 30th June 2016. No additional results collected from the SLALOM project [16][17][18].

2.2.3 SLA-Ready

The project ended on 31st December 2016. MUSA has adopted the SLA-Ready SLA Repository [19] populated in the DST-Decision module to compare the security features of the different Cloud providers. The repository served as a transparent, unprocessed dataset that can represent the state of the CSPs' Security controls. MUSA was invited to the *SLA-Ready Final Impact Workshop* organised in Brussels on 16th December 2016 in order to explain to cloud SMEs and stakeholders how SLA-Ready results were adopted in MUSA.

2.3 Standards for Cloud Computing service metrics

2.3.1 SUoM

In the interval between D7.6 and this deliverable no new version of the SUOM standard [21] was released.

2.3.2 NIST Performance Measurement Guide for Information Security (NIST SP 800-55)

This NIST Special Publication 800-55 [24] lists a set of useful security metrics that can be used to evaluate and benchmark different systems, including cloud-based environment. The document latest release was released on 2008.

The NIST SP 800-55 provides a guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. The document aims at providing an approach to help management decide where to invest in additional security protection resources or identify and evaluate non-productive controls.

It is worth noticing that the document describes not only a set of proposed metrics, but even the process to develop and implement security metrics. Moreover, it suggests how to use quantitative measurement to adequately justify security control investments.

2.3.3 CIS Security Metrics

The Center for Internet Security [25] provides a set of security benchmarks devoted to evaluating internet-oriented systems. The proposed benchmarks and security metrics can be adopted even in a cloud environment. The List of metrics and supported tools is available on the CIS benchmarks website [26].

2.4 Cloud security specific standards

2.4.1 NIST Cloud Computing Reference Architecture (NIST SP 500-292)

In the interval between D7.6 and this deliverable no new version of the NIST SP 500-292 [27] standard was released.

2.4.2 NIST Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53)

An Initial Public Draft of NIST SP 800-53, revision 5 [28], was released from NIST in August 2017. Being this a draft too novel for the MUSA project time schedule, the MUSA Framework and tools support revision 4 [29], which is stable.

2.4.3 NIST Cloud Computing Security Reference Architecture (NIST SP 500-299)

A draft of the NIST Cloud Computing Security Reference Architecture is available SP 500-299 [30]. The document aims at defining a framework that identifies a core set of Security Components to be implemented in a Cloud Ecosystem in order to secure the environment. The framework should provide, for each Cloud Actor, the core set of Security Components that fall under their responsibilities depending on the deployment and service models. Moreover, the framework aims at defining a security-centric formal architectural model that adds a security layer to the current NIST Cloud Computing Reference Architecture.

2.5 ISO/IEC JTC 1 SC 38

ISO/IEC JTC 1 SC 38 [2] is the standardization effort under ISO/IEC concentrating on the standards for Cloud Computing and Distributed Platforms. The Sub-committee is composed of national body delegations representing multi-national companies, governmental agencies, other software defining organizations (SDOs), and universities. The goal of SC 38 is to produce standards that will encourage, facilitate and stimulate the adoption, deployment and use of cloud computing. Rather than duplicating the standards development efforts of other SDOs, SC 38 affirms generally accepted standards from those SDOs, choosing rather to focus on cloud computing areas lacking standards or needing a common standard.

MUSA has tracked the ISO/IEC JTC 1 SC 38 standardization activities and developments to follow the guidelines and standards resulting from these efforts.

The initial focus of SC 38 was to focus on the standardization of a vocabulary and reference architecture around cloud computing. These efforts, *ISO/IEC 17788:2014 Cloud Computing Vocabulary* and *ISO/IEC 17789:2014 Cloud Computing Reference Architecture*, both finalized in 2014, were a joint project with the ITU represent a foundation upon which all subsequent SC 38 standards will be built. The second phase of work of SC 38 focuses on the interoperation and portability of cloud services and the results have been recently published. Major standards being developed in this phase include:

- A Cloud computing SLA Framework composed of four parts:
    - *ISO/IEC 19086-1:2016: Cloud Computing SLA framework: Overview and concepts.*
    - *ISO/IEC 19086-2 (under development): Cloud Computing SLA framework: Metric model*. The standard is still in final balloting process. It proposes a technical model for specifying cloud SLA metrics, which can be then used for automation, CSP comparison, service monitoring, and so forth.
    - *ISO/IEC 19086-3:2017: Cloud Computing SLA framework: Core conformance requirements.*
    - *ISO/IEC 19086-4 (under development): Cloud Computing SLA framework: Security and privacy* where approaches associated with the specification and the usage of Security SLAs are being discussed. *This upcoming standard acknowledges the importance of developing common SLOs and metrics for security SLAs* [31].

  The ISO/IEC 19086 framework provides a common vocabulary for use in Cloud Service Agreements and in their associated SLAs, which is very relevant for MUSA SLA Generation phase. As the development of these standards run in parallel to MUSA project and the security and metrics parts are still under development, it was not possible to adopt them and the NIST framework (see NIST standards above) was selected for the security service level objectives expression in the generated cloud SLAs.
- *ISO/IEC 19941:2017 Information technology - Cloud Computing - Interoperability and Portability and Guidelines* has been published in December 2017 and provides architectural models and common terminology and concepts for describing cloud interoperability, cloud data portability and cloud application portability and relates these models back to the Cloud Reference Architecture (ISO/IEC 17789).
- *ISO/IEC 19944:2017 Information technology - Cloud Computing - Cloud services and devices: data flow, data categories and data use* which provides a description of data flow between cloud services, cloud service customers, cloud services users and their devices. The standard also provides a scheme for the structure of data use statements to help cloud service customers understand, document and protect the privacy and confidentiality of their data.

Other relevant standards that were developed by SC 38 during the MUSA project lifetime and therefore not adopted in MUSA because the design decisions were made before they were published are:

- *ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*
- *ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*
- *ISO/IEC 27036-4:2016 Information security for supplier relationships. Guidelines for security of cloud services.*

2.6 Related Organisations and Initiatives

2.6.1 CSA

MUSA project has had a close relationship with Cloud Security Alliance (CSA) [32] due to the synergy of aims in developing tools and data that support the development of secure (multi-)cloud applications. The relationship has stalled due to the departure of a member of CSA staff and it is becoming increasingly difficult to elicit a response to enquiries, despite many attempts.

As an active group, there have been a number of new initiatives and updates to white papers and other documents. One of the most significant is the series of updates to the CSA security Guidance for Critical Areas of Focus in Cloud Computing 4.0 [33]. This is the first major upgrade since the guidance was first issued in 2011. There has been a major re-write with many new factors being included for the first time or getting increased emphasis. Hybrid Cloud implementations are now getting greater emphasis and micro-services and containers are considered for the first time.

The CSA STAR repository has been extended and complimented by the delivery of CSA STARWatch Cloud Security Management Application [34] in February of 2017. The STAR repository has been extended with a SaaS application that presents the Cloud Control Matrix (CCM) [35] and Consensus Assessments Initiative Questionnaire v3.0.1 (CAIQ) [36] in a database format. This enables users to manage their applications in line with the CSA Best Practices. Data obtained by CAIQ is used for demonstration purposes within the MUSA Risk and Decision Support Tool. The demonstration has been aided by CA holding a current licence for the core data. Other users of the MUSA DST will have to obtain their own licences. STARWatch has some service selection capabilities but it does not have the link between Risk, Security Controls and Decision Support that is part of the MUSA Framework. Discussions on the use of MUSA tools as part of CSA have now stalled, with CSA no longer responding to requests for meetings.

2.6.2 Cloud Watch 2

In this section we provide the list of cloud standards collected in the Cloud Standards guide [37] delivered by CloudWatch 2 EU project as part of its results. MUSA collaborated in the identification of these standards, putting the focus in those related to security. Note that we have included the links to the standards in the guide for the sake of clarity.

Table 1: Cloud standards in CloudWatch2 Guide adopted in MUSA

Standard in CloudWatch 2 Standards Guide	Standardisation Body	Adoption in MUSA
1. Avoiding vendor lock-in: Cloud standards for portability These standards relate to the application deployment modelling and Cloud Service selection support in MUSA.		
Open Virtualization Format (OVF)	Distributed Management Task Force (DMTF)	Not adopted in MUSA, but CAMEL.
Topology and Orchestration Services for Applications (TOSCA)	OASIS	Not adopted in MUSA, but CAMEL.
2. Interoperable Clouds: Cloud standards for Interoperability These standards relate to the application deployment execution in MUSA.		
a) Infrastructure as a Service cloud standards		
Open Cloud Computing Interface (OCCI)	Open Grid Forum	Not adopted in MUSA.
Cloud Infrastructure Management Interface (CIMI)	Distributed Management Task Force (DMTF).	Not adopted in MUSA.
Cloud Data Management Interface (CDMI)	The Storage Networking Industry Association (SNIA)	Not adopted in MUSA.
b) Platform as a Service cloud standards		
Cloud Application Management Protocol (CAMP)	OASIS	Not adopted in MUSA.
c) Software as a Service cloud standards		
No cloud specifics.	N/A	N/A
3. Secure Clouds: Cloud standards for security These standards relate to the security requirements specification and assurance in MUSA.		
ISO / EIC 27018 Code of practice for data protection controls for public cloud computing services	ISO	Adopted in MUSA.
NIST 800-53 Rev.4 Security Controls	NIST	Adopted in MUSA.
NIST Security Reference Architecture	NIST	Adopted in MUSA.
Cloud Controls Matrix (CCM) -	Cloud Security Alliance	Adopted in MUSA.

Open Certification Framework (OCF) -	Cloud Security Alliance	Not adopted in MUSA.
Cloud Trust Protocol (CTP) -	Cloud Security Alliance	Not adopted in MUSA.
CloudAudit	Cloud Security Alliance	Not adopted in MUSA.
Privacy Level Agreement	Cloud Security Alliance	Not adopted in MUSA.
EuroCloud Star Audit (ESCA)	EuroCloud	Not adopted in MUSA.
Data Security Framework	Open Data Center Alliance	Not adopted in MUSA.

2.6.3 CSCC

The Cloud Standards Customer Council's whitepapers[38] that were published in the period and taken into account in MUSA are the following:

- ***Public Cloud Service Agreements: What to Expect and What to Negotiate V2.0.1*** (August 2016) [39]. The guide complements the CSCC's *Practical Guide to Customer Service Agreements* whitepaper in the aspects of Security, Privacy and Data residency, being the Data residency the most novel part. The Data residency refers to location of data, movement of data across geographies and jurisdictions, and protection of that data against unintended access, as defined by the Object Management Group.
- ***Cloud Customer Architecture for Securing Workloads on Cloud Services*** (April 2017) [40]. This guide provides a practical reference to help architect, install, and operate the information security components of solutions built using cloud services. The document extends the high-level recommendations in the CSCC's *Security for Cloud Computing: Ten Steps to Ensure Success V2.0* and the CSCC's *Cloud Security Standards: What to Expect & What to Negotiate V2.0*. The guide is structured in 7 components of the CCSC architecture for security of cloud service solutions: 1. Identity and Access Management, 2. Infrastructure Security, 3. Application Security, 4. Data Security, 5. Secure DevOps, 6. Security Monitoring and Vulnerability, and 7. Security Governance, Risk and Compliance.
- ***Data Residency Challenges - A Joint Paper with the Object Management Group®*** (May 2017) [41]. This whitepaper puts the focus on data residency challenges of Cloud services and goes into detail on multiple data residency factors: Issues and Risks, Laws and Regulations, Applicable or Related Standards, Cloud Customer Needs and Challenges.
- ***Practical Guide to Cloud Computing Version 3.0*** (December 2017) [42]. This guide has recently been released and has not played a major part in MUSA design, although it may have been influential earlier in the project. Previous guides have not considered containers, hybrid clouds, serverless computing and microservices and had little value to MUSA beyond the more general architectural structures of SaaS, PaaS and IaaS. This guide is more clearly focussed on the technologies that underpin multi-cloud implementations and tools. Part of the guide considers cloud implementations and architectures and selection of approaches. There is a roadmap for cloud computing that advises on Selecting a cloud architecture, a clous supplier and takes an implementation from the fisrt steps of building the team through to managing the environment. Sadly like so many of the road map documents produced, it does not discuss retirement of an obsolete application.

2.6.4 MPAA

In D7.5 *Standards Analysis and Strategy Plan* it was noted that the significance of the Motion Picture Association of America (MPAA) [43] is based on their work in the area of content security. The best practices are freely available on the website 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.

There have been no significant developments for MUSA within MPPA since D7.5.

2.6.5 ENISA

Two main contributions from ENISA on cloud security [47] were published and studied in MUSA in the period:

1. The ***Exploring Cloud Incidents*** short paper [48]: The whitepaper explores the approaches as well as technical, organisational, legal and horizontal challenges of cloud forensics in the EU. Among the legal challenges, the report states that *to facilitate forensics activities, the CSPs should define the terms and conditions in the contracts*. The report recommends the SLAs to include clauses on forensics investigations like data access and procedures for forensics, as well as roles and responsibilities. The report particularly mentions that *Metrics (Service Level Objectives) to be included in the SLA could facilitate the forensics activities, and in particular metrics on implementation of logs and procedures, metrics on the effectiveness of incident resolution and metrics of efficiency of incident resolution*. This is directly linked with the work of MUSA on security metrics definition within cloud-based applications' SLAs based on providers' defined cloud SLAs. The MUSA use cases did not include the aspects of forensics but this is considered as future work beyond the project end.
2. ***Cloud Certification Schemes List (CCSL):*** In close collaboration with the European Commission and the private sector, ENISA developed a list of certification schemes [49] which could be relevant for potential cloud customers. The creation of this list is explicitly mentioned as a key action in the *European Cloud Strategy* [50]. The list complements a previous report by ENISA *Schemes for auditing security measures* [51] which gives an overview of a range of information security certification schemes used in different sectors.

   This directly fits the research on the MUSA Security Assurance Platform, particularly for the incident monitoring and reaction recommendations. The certification schemes will be studied to learn how the MUSA Assurance Platform can fit the diverse certifications to enhance its exploitation.

2.6.6 STRIDE

STRIDE is a classification scheme for classifying known threats. It forms part of the Microsoft Threat Modelling Process [52] . Although STRIDE is a proprietary process its use in MUSA Risk Assessment process would not be compromised since it depends on methodology and process that can be created specifically to support a software process such as the MUSA DST - Risk Analysis module.

STRIDE is an acronym using the first letter of the following categories:

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of privilege

This part of the threat modelling process has been implemented in MUSA to help manage the known threats identified by a DevOps Team expecting to select security risk aware services. The review of the risk and threat management section of the MUSA framework in deliverable D3.3 *Final security based discovery and composition* demonstrates how threats are classified.

Although the threat modelling process as a whole is quite dated, indeed Microsoft only have references on their site as a courtesy, STRIDE is no less valid in the MUSA scenario. It is of the correct weight for the purpose of threat classification in the context of Cloud Service Selection process and does not have the heavyweight approach of a methodology such as OCTAVE [53]. Changes to STRIDE need not result in changes to the MUSA framework. STRIDE is included here as a potential de-facto standard in some parts of the Risk Management Community.

2.6.7 OWASP

The OWASP risk rating methodology [54] was adopted in MUSA for establishing both technical and business impact factors of the threats within the DST-Risk Analysis module. OWASP was also adopted for the SLA Generator security assessment method. The methodology is a well-known best practice for assessing website security that can be easily adapted to the needs and characteristics of diverse case studies. It is important to note that MUSA Framework only adopted the methodology and not the resources in The Risk Rating Management Project [55] to handle and record the risk score into database. The management and storage of the risk scores is done in MUSA by the DST-Risk Analysis itself.

2.6.8 ROAM

ROAM is an acronym for a facilitation technique to evaluate risks in a Program Increment (PI) planning session [56] in the Scaled Agile Framework (SAFe) [57]. The characters in the acronym stand for:

- **R**esolved – the issue is no longer a concern.
- **O**wned – the issue needs further work and the owner will attempt to resolve it.
- **A**ccepted – some risks are facts or problems that must be understood and accepted.
- **M**itigated – a plan or solution can be identified to reduce the impact of this risk.

ROAM is included in this document for the first time, even though it is not an accepted standard but part of a framework. The inclusion is necessary since ROAM is an adapted, but integral part of classifying risk mitigation levels within the MUSA framework, particularly in the DST-Risk Analysis module. ROAM is unlikely to develop, but may be superseded if the risk management elements of Agile methodologies develop particularly with the current pressure to “shift-left” elements of Agile.

3 Standards and Best Practices Adopted

The following table summarises the standards and best practices adopted in MUSA Key Results (KRs) and work packages (WPs). Two of the adopted best practices, STRIDE and ROAM are risk oriented but also have relevance in an Agile methodology. Agile methodologies are integral in some of the tools developed in MUSA and the Kanban style interface to the MUSA framework is based on tools used to manage Agile development. Agile methodologies are generaly best practices and so far have not spawned new technical committees.

Table 2: Standards and Best practices adopted in MUSA

Standard/Best practice	Standards Body /Organisation	Status	Work Package, Key Result	Notes
ISO/IEC 17789	ISO	Standard Published	WP1, KR0 Framework architecture.	Definition of main roles in cloud architectures and basis for MUSA process roles.
ETSI TR 103 125 V1.1.1 (2012-11) technical report	ETSI	Standard Published	WP2, KR1 SLA Generator.	Definition of main roles in cloud SLA and recommendations for SLA specification.
WS-Agreement	OGF	Standard Published	WP2, KR1 SLA Generator	Language for machine-readable SLAs specification.
NIST Cloud Reference Architecture (NIST 500-292)	NIST	Standard Published	Considered as the reference for the cloud service models and architecture.	WP1, KR0 Framework architecture and glossary.
NIST SP 800-53 r4	NIST	Standard Published	WP2, KR1 Modeller & SLA Generator WP3, KR3 DST-Risk Analysis	Considered as the basis for the cloud services security controls description in CAMEL, Security SLA and Risk analysis.
CSA CAIQ	CSA	Standard Published	WP3, KR3 DST-Decision	Considered as the basis for the cloud services match-making.
STRIDE	Microsoft	Best practice Published	WP3, KR3 DST-Risk Analysis	Threats classification in Risk assessment follows the STRIDE model.
ROAM	Scaled Agile	Best practice Published	WP3, KR3 DST-Risk Analysis	Risk mitigation level assessment follows the ROAM model.

4 Relevant Standards for security in multi-cloud applications

Table 1 below gives a list of relevant standards for security-by-design and security assurance in (multi-)cloud. Some of them were adopted in MUSA, as described in previous section, and some are but no always adopted standards within the MUSA project

Table 3: Standards and Best practices relevant for security in multi-cloud applications

Standard	Standards Body	Relevance to MUSA
Cloud		
ISO/IEC 19086 Service Level Agreement (SLA) Framework and Terminology	ISO/IEC	Cloud SLA with security properties - WP2
ISO Cloud Reference Architecture (ISO/IEC 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.
ETSI SR 003 391, v2.1.1, Cloud Computing Interoperability and Security	ETSI	General reference for Cloud standards on Interoperability and Security.
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 SP 800-144,: Guidelines on Security and Privacy in Public Cloud Computing	NIST	Security and privacy aspects in public clouds.
NIST SP 500-291, Version 2, Cloud Computing Standards Roadmap	NIST	Cloud computing standards roadmap.
ISO/IEC 27001	ISO/IEC	Framework for information security management systems.
ISO/IEC 27002	ISO/IEC	Security controls.
ISO/IEC 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.

5 Conclusion

Security is a horizontal feature that cuts across applications and services to assure the safety and accuracy of technology. It is important that security threats and risks are considered early in any service or application development project. Agile methodologies frequently focus on user stories to develop a view of features and functions that users want. Users seldom suggest that security is included in user stories. Agile methodologies are an integral part of many organisations development strategy. Agile methodologies are unlikely to spawn technical committees as they are mostly best practices supported by methodologies and some tools. In the same context MUSA is unlikely to result in a new standards technical committee since it is an aggregator of secure services and it is the services, composition and security that will be the logical domains for any new standards body technical committees.

The standards landscape in relation to MUSA is a little confused, as noted in the Cloud Standards Coordination in D7.5 and D7.6. Each element in the MUSA framework has different standards and often there is an overlap for example, NIST and ISO security controls. Hence the standards observatory reviewed more than the standards adopted in MUSA. MUSA uses a wide variety of standards due to the wide variety of tools, best practices and technologies that it embraces. It is difficult in some cases to adopt a potentially relevant standard because it is being developed in parallel to MUSA.

The MUSA project considers that the strategy of any users would be to consider this report and the standards that are adopted in the MUSA framework within the scope of their domain. Adoption of standards should always be done in the context of the target market for some or all the tools, although this is sometimes difficult with standards that are immature or under development. Standards are important for flexibility and interoperability but they should not hamper or dictate functionality required by the users and the business.

References

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

[2] ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms. Available at: https://www.iso.org/committee/601355.html

[3] ETSI Network Functions Virtualisation (NFV). Available at: http://www.etsi.org/technologies-clusters/technologies/nfv

[4] Topology and Orchestration Specification for Cloud Applications Version 1.0, OASIS Standard, 25 November 2013. Available at: http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html

[5] CLOUDML. Available at: http://cloudml.org

[6] PaaSage EU project. Model Based Cloud Platform Upperware. FP7- ICT-2011.1.2. 2012-2016. Available at: www.paasage.eu/

[7] REMICS EU project, Available at: http://www.remics.eu

[8] ARTIST EU project. Advanced software-based service provisioning and migration of legacy software. FP7- ICT-2011.1.2, 2012-2015. www.artist-project.eu/

[9] 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/

[10] Cloud Application Modelling and Execution Language (CAMEL) and the PaaSage Workflow. In A. Celesti and P. Leitner (Eds.): ESOCC 2015 Workshops, CCIS 567, Springer, pp. 437-439, 201. DOI: 10.1007/978-3-319-33313-7.

[11] Rios, E., Iturbe, E., & Palacios, M. C. (2017). Self-healing Multi-Cloud Application Modelling.

[12] Open Grid Forum Published Documents. Available at: https://www.ogf.org/ogf/doku.php/documents/documents

[13] OASIS CAMP standard. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp

[14] WS-Agreement GFD.192 Available at: https://www.yumpu.com/en/document/view/21403326/gfd192-open-grid-forum

[15] SPECS Project. Secure Provisioning of Cloud Services based on SLA management. FP7- ICT-2013.1.5, 2013-2016. Available at: http://specs-project.eu/

[16] SLALOM Model Contract. Available at: http://slalom-project.eu/sites/slalom/files/content-files/article/SLALOM%20D2%202%20%2814Apr2016%29_v1.2.pdf

[17] SLALOM SLA Specification. Available at: http://slalom-project.eu/sites/slalom/files/content-files/article/SLALOM%20D3.3_v1.0.pdf

[18] Cloud SLA Metrics Based on the SLALOM Specification and Reference Model v1. Available at: http://www.slalom-project.eu/sites/slalom/files/content-files/article/Cloud%20SLA%20Metrics%20Based%20on%20the%20SLALOM%20Specification%20and%20Reference%20Model%20v1.pdf

[19] SLA-READY Repository. Available at: http://www.sla-ready.eu/sla-repository

[20] SLA-READY CRM. Available at: http://www.sla-ready.eu/common-reference-model

[21] SUoM. Available at: https://opendatacenteralliance.org/docs/Standard_Units_of_Measure_For_IaaS_Rev1.1.pdf

[22] SUoM - Provider Assurance Usage Model. Available at: https://www.opendatacenteralliance.org//docs/Provider_Assurance_Rev2.0.pdf

[23] SUoM - Identity Management Interoperability Guide. Available at: https://www.opendatacenteralliance.org//docs/Identity_Management_Interoperability_Guide_Rev1.0_b.pdf

[24] Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Revision 1. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

[25] Center for Internet Security. Available at: https://www.cisecurity.org

[26] Center for Internet Security Free Benchmarks. Available at: https://learn.cisecurity.org/benchmarks

[27] NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292. Available at: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505

[28] Initial Public Draft of Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 5. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[29] Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4. Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[30] Draft of NIST Cloud Computing Security Reference Architecture, NIST Special Publication 500-299. Available at: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

[31] Luna, J., Suri, N., Iorga, M., & Karmel, A. (2015). Leveraging the potential of cloud security service-level agreements through standards. IEEE Cloud Computing, 2(3), 32-40.

[32] CSA Cloud Security Alliance. Available at: https://cloudsecurityalliance.org

[33] CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/guidance/#_overview

[34] Cloud Security Alliance Announces General Availability of STARWatch Cloud Security Management Application. Available at: https://cloudsecurityalliance.org/media/news/cloud-security-alliance-announces-general-availability-of-starwatch-cloud-security-management-application/

[35] Cloud Controls Matrix Working Group, Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

[36] Consensus Assessments Initiative Questionnaire v3.0.1 (9-1-17 Update), Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/

[37] Cloud Standards guide by CloudWatch 2 project. Available at: http://www.cloudwatchhub.eu/cloud-standards-guide

[38] Cloud Standards Customer Council's Resource Hub. Available at: http://www.cloud-council.org/resource-hub.htm

[39] Public Cloud Service Agreements: What to Expect and What to Negotiate V2.0.1, Cloud Standards Customer Council. Available at: http://www.cloud-council.org/deliverables/cloud-security-standards-what-to-expect-and-what-to-negotiate.htm

[40] Cloud Customer Architecture for Securing Workloads on Cloud Servicesm, Cloud Standards Customer Council. Available at: http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-securing-workloads-on-cloud-services.htm

[41] Data Residency Challenges A Joint Paper with the Object Management Group®, Cloud Standards Customer Council. Available at: http://www.cloud-council.org/deliverables/data-residency-challenges.htm

[42] Practical Guide to Cloud Computing Version 3.0, Cloud Standards Customer Council. Available at: http://www.cloud-council.org/deliverables/practical-guide-to-cloud-computing.htm

[43] CSCC. Available at: http://www.cloud-council.org

[44] CSCC Security for Cloud Computing. Available at http://cloud-council.org/resource-hub.htm/

[45] CSCC Cloud Security Standards. Available at: http://cloud-council.org/resource-hub.htm/

[46] MPAA best practices. Available at http://www.fightfilmtheft.org/best-practice.html

[47] ENISA Cloud Security. Available at: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

[48] Exploring Cloud Incidents , ENISA, June 2016. Available at: https://www.enisa.europa.eu/publications/exploring-cloud-incidents/at_download/fullReport

[49] Cloud Computing Certification - CCSL and CCSM, ENISA. Available at: https://resilience.enisa.europa.eu/cloud-computing-certification

[50] European Cloud Strategy, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[51] Schemes for auditing security measures, ENISA, 2013. Available at: https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures/at_download/fullReport

[52] The STRIDE Threat Model. Available at: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[53] Alberts, Christopher, et al. "Introduction to the OCTAVE Approach." *Pittsburgh, PA, Carnegie Mellon University* (2003).

[54] OWASP Risk Rating Methodology. Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[55] OWASP The Risk Rating Management Project . Available at: https://github.com/mohammadfebrir/owasp-riskrating.git

[56] PI Planning within SAFe Framework by Scaled Agile. Available at: http://dev.scaledagileframework.com/pi-planning/

[57] SAFe Framework by Scaled Agile. Available at: http://www.scaledagileframework.com/what-is-safe/

[58] ETSI Cloud Standards Coordination (CSC). Available at: http://csc.etsi.org/

[59] NIST SP 500-317 DRAFT, http://www.nist.gov/itl/cloud/upload/sp500-317_v01-draft.pdf

[60] Exploring Cloud Incidents, ENISA, June 2016. Available at: https://www.enisa.europa.eu/publications/exploring-cloud-incidents/at_download/fullReport

[61] CloudWATCH project. Available at: http://cordis.europa.eu/project/rcn/110185_en.html

[62] CloudWATCH2 project. Available at: http://cordis.europa.eu/project/rcn/196626_en.html

[63] CloudWATCH project's deliverable D4.3. Available at: http://www.cloudwatchhub.eu/sites/default/files/D4.3_Final-report-on-Cloud-standards-profile-development_vFinal-Update1_0.pdf

[64] Cloud Industry Forum. Available at: https://www.cloudindustryforum.org

[65] TMF, TM Forum, Available at: https://www.tmforum.org

[66] OGF, Open Grid Forum Available at: https://www.ogf.org/ogf/doku.php

[67] OASIS Standards Organisation, Available at: https://www.oasis-open.org

[68] ODCA Open Data Center Alliance, Available at: http://www.opendatacenteralliance.org

[69] OAuth 2.0 Next evolution of the OAuth protocol Available at: http://oauth.net/2/

[70] SAML 2.0 Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[71] ISO 27001/2 standard. Available at: http://www.27000.org

[72] NIST 800-5r4 Available at: http://csrc.nist.gov/publications/PubsFL.html

[73] ISO 27002 standard. Available at: http://www.27000.org

[74] ISO 27017 standard. Available at: http://www.iso27001security.com/html/27017.html

[75] Open Grid Forum's OCCI. Available at: http://occi-wg.org

[76] NIST Cloud Reference, Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505

[77] NIST Cloud computing service metrics description. Available at: http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf

[78] 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/

[79] 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

[80] ENISA Cloud Security Guide for SMEs. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes

[81] ENISA SME Guide Tool: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/sme-guide-tool

[82] ENISA Cloud Computing Certification. Available at: https://resilience.enisa.europa.eu/cloud-computing-certification

[83] ENISA, Cloud Standards and Security. Available at: https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf

[84] 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.

[85] 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

[86] 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.

[87] Cloud Service Level Agreement Standardisation Guidelines. Available at: http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[88] ISO/IEC 19086 project. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902

[89] CSA's GRC stack. Available at: https://cloudsecurityalliance.org/research/grc-stack/#_overview

[90] 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

[91] The European Cloud Partnership (ECP). Available at: http://ec.europa.eu/digital-agenda/en/european-cloud-partnership.

[92] 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

[93] 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

[94] 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

[95] 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

[96] 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. .

[97] 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 .

[98] CloudWATCH Cloud Certification on Guidelines and Recommendations. Available at: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Cloud_certification_guidelines_and_recommendations_0.pdf

[99] 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

[100] Guidelines on Security and Privacy in Public Cloud Computing, NIST SP 800-144. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[101] Cloud Computing Standards Roadmap, NIST SP 500-291 revision 2. Available at:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf

Appendix A. MUSA motivation and background

The main goal of MUSA project 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.

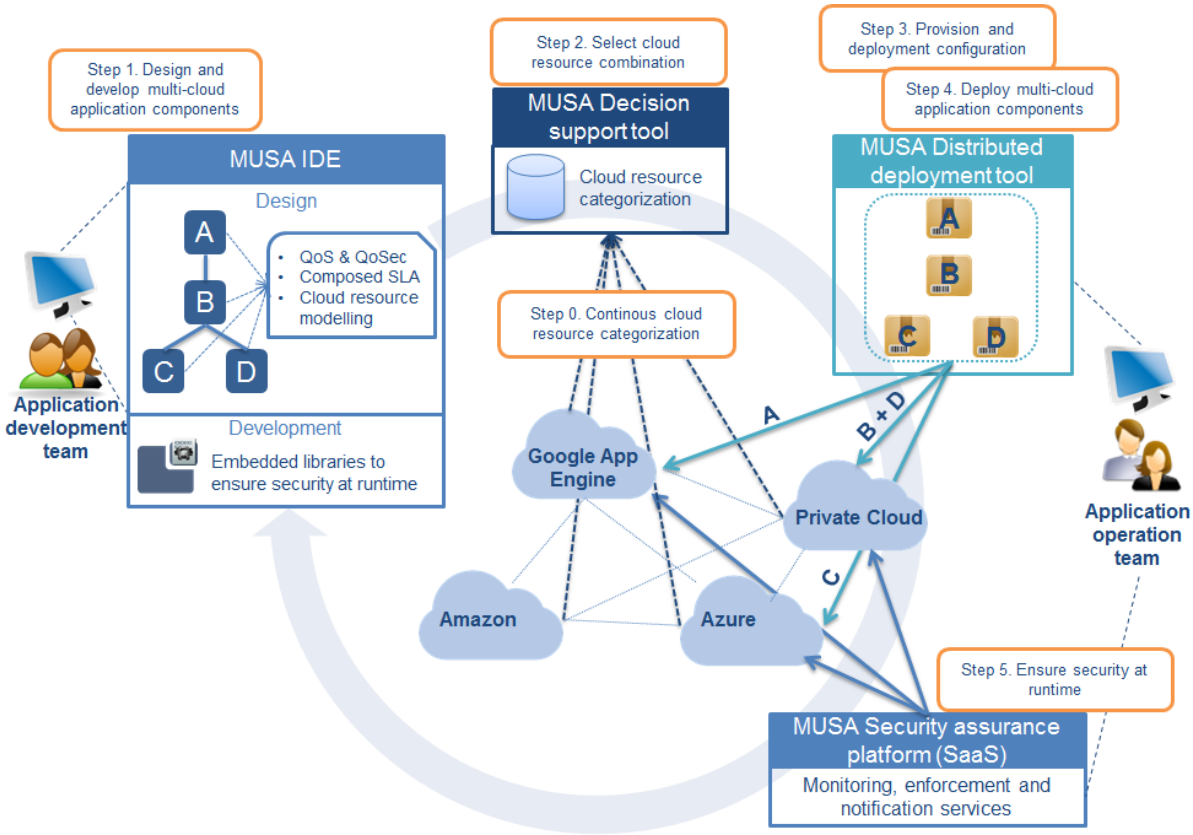

Figure A.1: MUSA overall concept

MUSA framework combines 1) a preventive security approach, promoting Security by Design practices in the development and embedding of 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 security measures to be embedded and aligned with reactive security measures.