decide

MULTICLOUD APPLICATIONS TOWARDS
THE DIGITAL SINGLE MARKET

Deliverable D5.1

ACSmI requirements and technical design

Editor(s):	Marisa Escalante
Responsible Partner:	TECNALIA
Status-Version:	V3.0 - Final
Date:	31/05/2017
Distribution level (CO, PU):	Public

Project Number:	GA 731533
Project Title:	DECIDE

Title of Deliverable:	ACSmI requirements and technical design
Due Date of Delivery to the EC:	31/05/2017

Workpackage responsible for the Deliverable:	WP5 – Continuous cloud services mediation
Editor(s):	TECNALIA
Contributor(s):	Lena Farid (FhG) Peter Deussen (FhG) Antony Shimmin (AIMES) Pieter Gryffroy (Time.lex) Anna Shevchenko (CB) Maria Jose Lopez (TECNALIA) Marisa Escalante (TECNALIA) Gorka Benguria (TECNALIA) Leire Orue-Echevarria (TECNALIA) Juncal Alonso (TECNALIA) Iñaki Etxaniz (TECNALIA)
Reviewer(s):	Jose Antonio Flaño (ARSYS) Miguel Ángel Pérez (ARSYS)
Approved by:	All Partners
Recommended/mandatory readers:	WP2, WP3 and WP4

Abstract:	Requirements analysis, technical detailed design and initial mock-ups of the Advanced Cloud Service meta-Intermediator (ACSmI). This document will also present the prioritization of the functionalities that will be implemented in each version of the ACSmI based on the requirements and needs expressed in the DECIDE use case validations in WP6. This deliverable is the result of T5.1 – T5.5.
Keyword List:	CSP´s services, Cloud services, Contracting, Service discovery, CSP monitoring

Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/
Disclaimer	This document reflects only the author's views and the Commission is not responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	20/01/2017	TOC	TECNALIA
v0.2	27/02/2017	Inclusion of requirements in section 4	TECNALIA; Time.lex; FhG; CloudBroker
V0.3	10/03/2017	Integration of the requirements section 4	TECNALIA
V0.4	3/04/2017	Section 2 – first version	CloudBroker; Time.lex; FhG
V0.5	5/04/2017	Section 3	TECNALIA
V0.6	12/04/2017	Final version of the section 4	TECNALIA; Time.lex; FhG; CloudBroker
V0.7	21/04/2017	Section 5.- First Version Section 6 .- First Version Section 7.- First Version	TECNALIA; Time.lex; FhG; CloudBroker; AIMES
V0.8	04/05/2017	Section 6.- Reviewed Section 7.- Reviewed	TECNALIA; FhG; CloudBroker;
V0.9	15/05/2017	Ready for internal review	TECNALIA
V1.0	23/05/2017	Amended version after internal review	TECNALIA
V2.0	29/05/2017	Final version	TECNALIA
V3.0	30/05/2017	Ready for submission	TECNALIA

Table of Contents

Table of Contents 5
List of Figures 7
List of Tables 7
Terms and abbreviations 8
Executive Summary 9
1 Introduction 10
1.1 About this deliverable 10
1.2 Document structure 10
2 State of the Art 11
2.1 Solutions for Cloud Service Brokers 11
2.1.1 ACSmI Functionalities Gap Analysis 14
2.1.1.1 Features that do not exist in the available solutions 14
2.1.1.2 Features that exist in the available solutions but should be extended for ACSmI ... 15
2.2 Standards, and Certification Schemes with Cloud Relevance 15
2.2.1 Criteria 15
2.2.2 Standards Analysis 17
2.2.2.1 Concepts and Vocabulary 17
2.2.2.2 Service Levels and Service Level Monitoring 17
2.2.2.3 Cloud Security 18
2.2.2.4 Cloud Interoperability and Federation 20
2.3 Legislation 22
2.3.1 ACSmI alignment with legislation 22
3 Main actors of the ACSmI 24
4 General Description of the Solution 25
4.1 Main objectives of the ACSmI 25
4.2 High level architecture 26
5 ACSmI Requirements 29
5.1 CSPs service discovery and management 29
5.1.1 Functional requirements 29
5.2 Dynamic monitoring of CSPs SLAs 32
5.2.1 Functional requirements 33
5.3 Security management 37
5.3.1 Functional requirements 37
5.4 Legislation compliance and monitoring 40
5.4.1 Functional requirements 40
5.5 Business modelling implementation 41

5.5.1 Functional requirements 41
5.6 Non Functional requirements 46
6 ACSmI Design........ 47
6.1 CSPs service discovery and management 47
6.1.1 Main functionalities........ 47
6.1.2 Component Diagram 47
6.2 Dynamic monitoring of CSPs SLAs 49
6.2.1 Main functionalities........ 49
6.2.2 Component Diagram 49
6.3 Security management 50
6.3.1 Main functionalities........ 50
6.3.2 Component Diagram 51
6.4 Legislation compliance and monitoring 52
6.4.1 Main functionalities........ 52
6.4.2 Component Diagram 53
6.5 Business modelling implementation 54
6.5.1 Main functionalities........ 54
6.5.2 Component Diagram 54
7 Technologies to be used and deployment options 56
8 Conclusions........ 58
9 References........ 59

List of Figures

Figure 1: Main functionalities of ACSmI 25
Figure 2: ACSmI High Level Architecture........ 26
Figure 3: Service Management external component diagram 48
Figure 4: Service Discovery Management internal component diagram 48
Figure 5: SLA Monitoring External component diagram 49
Figure 6: SLA Monitoring Internal component diagram........ 50
Figure 7: Security Management external component diagram 51
Figure 8: Security Management internal component diagram 52
Figure 9: Legislation compliance external component diagram 53
Figure 10: Legislation Compliance internal component diagram........ 53
Figure 11: Business Model Management external component diagram........ 54
Figure 12: Business Model Management internal component diagram 55
Figure 13: Server Virtualisation across company sizes [43] 57

List of Tables

Table 1: Solutions for Cloud Services Brokers 11
Table 2: Standards related to Concept and Vocabulary 17
Table 3: Standards related to Service Levels and Service Level Monitoring 17
Table 4: Standards related to Cloud Security........ 18
Table 5: Standards related to Cloud Interoperability and Federation........ 20

Terms and abbreviations

ACSmI	Advanced Cloud Service meta Intermediator
CAMP	Cloud Application Management for Platforms
CCM	Cloud Controls Matrix
CDMI	Cloud Data Management Interface
CIMI	Cloud Infrastructure Management Interface
CRUD	Create, Read, Update and Delete
CSA	Cloud Security Alliance
CSC	Cloud Standards Coordination
CSP	Cloud Service Provider
DBaaS	DataBase as a Service
DMTF	Distributed Management Task Force
DoA	Description of Action
DPaaS	Data Protection as a Service
EC	European Commission
ETSI	European Telecommunication Standardization Institute
GDPR	General Data Protection Regulation
HaaS	Hardware as a Service
HPC	High Performance Computing
IaaS	Infrastructure as a Service
IEC	International Electro-technical Commission
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ITU-T	International Telecommunication Union – Standardization Sector
KR	Key Result
MCSLA	Multi-Cloud Service Level Agreement
NFR	Non-Functional Requirement
OASIS	Organization for the Advancement of Structured Information Standards
OCCI	Open Cloud Computing Interface
OGF	Open Grid Forum
PLA	Privacy Level Agreement
QoS	Quality of Service
SaaS	Software as a Service
SDO	Standards Development Organisation
SLA	Service Level Agreement
SNIA	Cloud Data Management Interface
TOSCA	Topology and Orchestration Specification for Cloud Applications
WS-Agreement	Web Services Agreement

Executive Summary

The Advanced Cloud Service (meta-) intermediator (ACSmI) will provide means to assess continuous real time verification of the cloud services non-functional properties fulfilment and legislation compliance enforcement. ACSmI will also provide a cloud services store where developers can easily access centrally negotiated deals of compliant and accredited services and applications developed by the software sector.

This document contains the requirements and the design for ACSmI in the context of the DECIDE project. This document reflects the main interactions between other DECIDE KRs, mainly with OPTIMUS and ADAPT.

The main innovations of the tool detailed in this deliverable are:

- ACSmI will be solution centric as it will be able to discovery services from a range of services available in a registry; always making sure that the best combination for the user (i.e. OPTIMUS Tool and ADAPT tool) is met, while ensuring the integrity and security of the overall ACSmI solution.
- ACSmI is resource centric, providing flexible and opportunistic choices as well as continuous service governance, but ACSmI will intermediate not only resources provisioning services (HaaS) but also DBaaS, DPaaS, identity management as a service, Storage as a service as well as generic SaaS such as calendar, email, Content Management Systems.
- ACSmI will provide the means to set up a dynamic validation of legal solutions (contractual and policy framework) as the services registered will be legally assessed prior to the operation phase periodically checked the validity according to the results of continuous legal assessment.
- ACSmI will also be able to ensure the governance and overall quality of the service provision to the customer by continuously monitoring the fulfilment of the SLAs as well as propagating the legislation changes.

This design document is organized in the following manner. Section 1 is an introduction of the document. Section 2 provides an analysis of the existing solutions and their relation with the ACSmI. Section 3 describes the overall solution. Section 4 presents the ACSmI requirements. Section 5 lists the ACSmI actors. Sections 6 focuses on the design of the different components expected for the ACSmI. Section 7 presents additional features, the deployment option and technology to be used. Finally, section 8 presents the conclusions and future work.

1 Introduction

1.1 About this deliverable

The present document aims to develop further the initial design foreseen for the ACSmI tool (KR4).

This document contains the requirements and the design for ACSmI in the context of the DECIDE project. This document reflects the main interactions between other DECIDE KRs, mainly with OPTIMUS and ADAPT.

1.2 Document structure

This work starts with an analysis of the state of the art in three major topics: 1) solutions related to cloud service brokers, 2) standards and certifications and 3) legislation. For the first topic, we have analysed open source brokers as well as commercial cloud service brokers identifying which are the ACSmI functionalities that are not covered by these solutions. For the second issue, we have analysed a number of standards in order to understand and prioritize the standards the ACSmI must be aligned to. Finally, for the third theme of interest, we have analysed different legislation matters and initiatives on privacy, SLAs, and security that are of concern to the ACSmI.

The document then proceeds with the description of the main objectives of the ACSmI tool and a general description of its functionalities in Section 3. In the same section, the main components are presented with a brief explanation of what each module shall cover. In section 4, the list of DECIDE actors involved in ACSmI is detailed.

The ACSmI requirements are described in section 5. These requirements are elicited taken into account the five important components of the general architecture. The requirements have a unique identifier accompanied by the description of the requirement. In order to maintain the coherence in the whole project, references with the functionalities described in the deliverable D2.1 of DECIDE [1] have been included.

Based on the requirements elicited, section 6 compiled the functionalities that each component are expected to comply with, supported by the corresponding component diagrams. This allows us to understand the interaction of the different components both internally and externally.

Finally, the approach to be followed to deploy the ACSmI, and the technologies to be used are described in section 7. This section shall be coherent with the rest of the DECIDE framework.

2 State of the Art

2.1 Solutions for Cloud Service Brokers

Currently there exist multiple solutions for cloud service brokers on the market. The respective market is projected to grow further since there is a high demand for the cloud services and respective value-added services. To give an overview of the solutions currently available, the chapter will list and assess some cloud service brokerage companies and outline briefly the respective solutions they provide. For the reader's convenience, the solutions will be overviewed in a tabular form.

Table 1: Solutions for Cloud Services Brokers

Solution	Short Description
Cloudmore [2]	Cloudmore provides a way to procure, deploy and consume IT services. Cloudmore enables customizable IT automation, distributed control and relevant cost reconciliations that lower operational overhead and increase business agility [2] Additional characteristics are listed below: Focus on IT management for businesses; • Allows cloud store creation for customers to offer cloud automation to IT and business customers; • Multiple cloud services integrated; • Customers can integrate their own services.
Activeeon [3].	Activeeon is an open-source solution. The company focuses on consulting and project business [3]. Additional characteristics are listed below: • All major cloud protocols supported. • Cloud Automation support. • Workflow and scheduling included. • Parallel scientific toolbox supported: Cluster/Grid & Desktop MATLAB, Scilab & R readily deployed that is helpful for multiple researchers who are users of Activeeon. However, Activeeon is focused on French companies.
Nimbix [4]	Architecture of the solution is not disclosed, but expected to cover the full stack for cloud management. The solution offered includes pure high performance computing (HPC) cloud built for volume, speed and simplicity. The solution allows users to build, compute and visualize process. [4] Additional characteristics are listed below: • Focus on HPC clouds. • Software solutions in a cloud for multiple industries are provided. • API to allow portals/workflow solutions to interconnect. However, there is no transparency on supported infrastructure provided.

Solution	Short Description
Gompute [5]	The solution offers complete stack for cloud management in a modular way. [5] Additional characteristics are listed below: • Remote visualization. • Automated workflows. • HPC data stager. • Set of ready to use applications. • Own supercomputing centre. However, there is no transparency on supported infrastructure provided. Also, the pricing is not transparent.
CycleComputing [6]	Cycle computing offers full stack for cloud management. However, it is not transparent in terms of architecture, available software and use cases. [6] Additional characteristics are listed below: • CycleServer is a single management and submission interface for all grid activities. • Support for Condor (with GridEngine, Torque and Hadoop coming soon). However, there is no transparency on supported infrastructure provided.
Nice [7]	NICE empowers Grid & Cloud infrastructures by increasing usability and user-friendliness, without sacrificing flexibility and control. It provides portal and visualization capabilities for running applications on cloud and grid infrastructures. Provides Universal and flexible access to grid infrastructure. [7]
UberCloud [8]	A marketplace initiative. UberCloud provides users instant access to CAE software deployed onto various clouds. Multiple resource providers such as Amazon are represented on the Marketplace together with the scientific and engineering solutions. [8] Additional characteristics are listed below: • Marketplace. • Proven by 155 conducted experiments. • Allows users to access multiple apps deployed onto multiple clouds.
Fortissimo [9].	A marketplace initiative. The initiative is providing different applications running on HPC cloud infrastructure. One-stop-shop availability greatly simplifies access to advanced simulation, particularly to SME. Fortissimo includes over 50 experiments. It has 45 core partners including manufacturing companies, application developers, domain experts, IT solution providers and HPC cloud service providers from 14 countries. Hardware, expertise, applications, visualization and tools easily available and affordable on pay-per-use. The Fortissimo project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 609029. The Fortissimo 2 project has received funding from the European Union's Horizon 2020 research and

Solution	Short Description
	innovation programme under grant agreement No 680481 [9].
Extreme Factory [10] [11]	Extreme factory is a Bull and Atos company subsidiary. It has 4 configurations available: shared public, reserved public, private on-site, private hosted. Extreme factory offers computing portal with work environment customized for a user. [10] Additional characteristics are listed below: • Access to supercomputer for any size of business; • Focused on Bullx^{TM} Super Computers [11]; • Large number of European HPC specialists; • Remote visualizer (XRV).
Rescale [12]	Rescale is an American based company supported by Amazon and series of US investors. It has large number of applications available and large number of reference success stories. [12] Additional characteristics are listed below: • Series of industry partnerships. • Supporting Cloud Engine. • Number of applications. However, Rescale supports only Amazon infrastructure. In addition, it is US-focused.
CompatibleOne [13]	CompatibleOne is an open source cloud-aware software platform which enables organizations to operate Cloud Services Brokerage by making fully interoperable any cloud resources such as IaaS including Amazon, Azure, CloudSigma, Dimension Data, Joyent, Go Grid, HPCloud, RackSpace, OnApp, Softlayer and VMware vCloud, and PaaS providers including CloudFoundry and OpenShift [13].
Jamcracker [14]	The Jamcracker Platform is a comprehensive cloud services broker, cloud services management and cloud governance platform, including cloud services provisioning, policy management, cloud cost management, and operations management. Jamcracker enables organizations to create, deliver, and manage multi-cloud services and implement a cloud-enabled business model for offering, delivering, supporting and billing for multi cloud services. The Platform offers flexibility and scalability, with a multi-tiered, multi-tenant architecture, RESTful APIs and integration frameworks [14].
ComputeNext [15]	ComputeNext is an award-winning Cloud Marketplace Platform provider based in Redmond, WA. They empower consumers, vendors, and distributors of cloud services to connect and transact in a transparent and near real-time service delivery model. Specialties include Cloud Computing, Cloud Brokerage, Cloud Marketplace Platform, Federation, Iaas SaaS Marketplace, and Cloud Kiosk. [15]
Cloud28+ [16]	Cloud28+ is a federation of European Cloud Service Providers, Resellers, Independent Software Vendors (ISVs), and government entities coming together for information exchange, business development and providing an online Service

Solution	Short Description
	Hub of trusted cloud services and enterprise apps. Cloud28+ allows a fair comparison of available services vs. customer requirements, thanks to its homogenous semantic description of services, all included in the same catalogue. Cloud28+ brokering model results in creating a direct link between customer and supplier. The Cloud28+ community currently includes more than 400 members, with a catalogue of more than 1400 services. [16]
CloudBroker [17]	CloudBroker GmbH is a Swiss company providing services in the IT domain, in particular consulting, brokering, software development, project realization, distribution and selling in the area of cloud, grid and high performance computing. Its flagship product the CloudBroker Platform, is middleware and application store for compute intensive applications in the cloud. It works on different public and private clouds and high-performance computing (HPC) infrastructures and can be accessed through any web browser and through different application programming interfaces (APIs). [17] The main features provided by the Platform are the following: • Providing access to multiple clouds and HPC infrastructures. • Software deployment onto different cloud and HPC infrastructures. • Cloud instances management (including getting SSH access, Cloud-Init usage, etc.). • Running jobs on different clouds.

2.1.1 ACSmI Functionalities Gap Analysis

Taking into account WP5 description, ACSmI will be able to ensure the governance and overall quality of the service provisioning to the customers by **continuously monitoring the fulfilment of the SLAs** as well as propagating the legislation changes. ACSmI will be also able to **discovery from a range of services available;** always making sure that the NFRs of the end user are met. ACSmI will provide the means to set up a **dynamic validation of legal solutions** (contractual and policy framework) as the services registered will be legally assessed prior to the operation phase periodically checked the validity according to the results of **continuous legal assessment**.

Although a number of important features are already implemented for some of the solutions mentioned in the previous section, there are still some gaps that should be covered.

The gaps can be divided into two groups:

- Features that do not exist yet on the existing solutions;
- Features that exist on the existing solutions that, however, should be extended to be applied to ACSmI.

Both groups will be overviewed in this section. The detailed requirements are covered in section 4.

2.1.1.1 Features that do not exist in the available solutions

Such features are related to security, monitoring and control, and contracting and legal issues.

1. **Security:**

- Data encryption.
- Custom API access.

- Client data backup and archiving.

2. **Monitoring and control:**
   - CSP SLA monitoring.
   - Alarm system in case of SLA violation or a cloud service is non-operational; prohibiting to use non-operational clouds.
   - Intelligent "Advisory System" to provide recommendations as for services to be used.
3. **Contracting:**
   - Indicate how to contract services with each CSPs. Check if there are any procedures to get access to a service; if yes - the procedures are to be described to users.
   - Managing contract with the CSPs and Users

2.1.1.2 Features that exist in the available solutions but should be extended for ACSmI

For this case, the list is provided below.

1. **Billing:**
   - Functionality to charge a user in background for service usage.
   - Functionality to provide a user with billing details.
   - Functionality to provide a user with periodical invoices.
   - Functionality to provide a user with usage reports.
2. **Cloud Service Registry:**
   - Cloud service registry with multiple resources to be available for usage. The existing solutions of cloud repositories will be extended to contain various parameters available for DECIDE services, e.g. cloud availability, legal aspects and so on
3. **Security:**
   - Communication layer security
   - Authentication and policy and roles management

2.2 Standards, and Certification Schemes with Cloud Relevance

A large number of standards on Cloud Computing have been produced by various Standards Development Organisations (SDOs) during the last years. European experts have claimed the existence of a “jungle of standards” and various initiatives have been launched to cut through the supposed dense woods. In particular, the European Telecommunication Standardization Institute (ETSI) has conducted the so-called Cloud Standards Coordination (CSC) [18] action on behalf of the European Commission. The report [19] describes the results of CSC phase 2.

There are other sources available listing and comparing standards related to Cloud Computing, most notably the following:

- The cloud-standards.org website [20] provides a comprehensive list of SDOs and standards.
- The CloudWatch2 project maintains an excellent review of a number of standards on its CloudWatchHub website [21].

In this section, we will provide an analysis and prioritisation of standards on Cloud Computing which are relevant for the DECIDE project.

2.2.1 Criteria

Based on the CSC phase 2 report [19] we are going to assess the relevance of standards according to the following criteria:

- Nature: We have considered standards approved by an SDO only.
- Maturity: Only standards already published have been considered with one exception (see the entry on ISO/CD 19086-2 below)
- Topics: Standards of the following topics are most relevant for the further development of the ACSmI:
    - Generic standards on Cloud concepts and vocabulary.
    - Service level agreements and service level monitoring.
    - Cloud interoperability and Cloud federation with regard to Cloud service discovery and aggregation.
    - Security related aspects such as federated identity management.

The following list does not provide a final selection of the standards being used (or are relevant to) the ACSmI component, but aims to provide an overview on the most relevant standards and a basis for further research.

2.2.2 Standards Analysis

2.2.2.1 *Concepts and Vocabulary*

Table 2: Standards related to Concept and Vocabulary

Standard	SDO	Summary	Relevance
ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary [22]	ISO/IEC ITU-T	Provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. The standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).	These standards provides an internationally agreed terminology for cloud computing. Terms and definition defined in this standard shall be used throughout the DECIDE project.
ISO/IEC 17789:2014: Information technology -- Cloud computing -- Reference architecture [23]	ISO/IEC ITU-T	The standard specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships	

2.2.2.2 *Service Levels and Service Level Monitoring*

Table 3: Standards related to Service Levels and Service Level Monitoring

Standard	SDO	Summary	Relevance
ISO/IEC 19086-1:2016 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts [24]	ISO/IEC	ISO/IEC 19086-1:2016 seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud SLAs. It specifies an overview of cloud SLAs, an identification of the relationship between the cloud service agreement and the cloud SLA, concepts that can be used to build cloud SLAs, and terms commonly used in cloud SLAs.	The standard provides a comprehensive overview on Cloud service level and quality objectives and is thus a suitable reference for the metrics to be considered for the development of ACSmI.
ISO/CD 19086-2: Information technology --	ISO/IEC	The standard provides a formal definition of the	The standard defines a model for metrics for

Standard	SDO	Summary	Relevance
Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model (Committee Draft) [25] Remark. Part two of ISO/IEC 19086 is currently under ballot for a "Draft International Standard" and expected to be published in 2018.		term SLA metric.	Cloud service levels that has a machine-readable representation. Such a model is needed to develop a scheme for service discover and composition and to derive associated monitoring objectives.
Web Services Agreement (WS-Agreement) [26]	OGF	Describes Web Services Agreement Specification (WS-Agreement), 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 compound 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.	The standards describes schema for service level agreements alternative to the one given in [25], with focus on web services. It may be used in conjunction with [24].

2.2.2.3 Cloud Security

Table 4: Standards related to Cloud Security

Standard	SDO	Summary	Relevance
ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [27]		The standard formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called 'information security risks' in the standard). The ISMS ensures that the	The ISO/IEC 27000-series is the most influential set of standards on security for information and communication systems. Of particular relevance are [28] and [29] addressing cloud computing and the

Standard	SDO	Summary	Relevance
		security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts.	protection of personally identifiable information, respectively, [27] and [30] are listed as background material.
ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls [30]	ISO/IEC	The standard is a popular, internationally-recognized standard of good practice for information security.	
ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services [28]	ISO/IEC	This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002.	
ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors [29]	ISO/IEC	The standard is a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for organizations for implementing commonly accepted PII protection controls	
Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union [31]	CSA	The Privacy Level Agreements (PLAs) are intended to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the cloud service provider will maintain.	The standard provides a complementary view on cloud security that takes into account the General Data Protection Regulation of the EC
Cloud Controls Matrix [32]	CSA	The standard is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The Cloud Controls Matric (CCM) provides a controls framework that gives detailed understanding of security concepts and principles	Comprehensive table of controls to ensure/enhance security of cloud services. Complementary to the ISO/IEC 27000-series (see above)

Standard	SDO	Summary	Relevance
Clout Trust Protocol Data Model and API [33]	CSA	The specification is designed to be a mechanism by which cloud service customers can ask for and receive information related to the security of the services they use in the cloud, promoting transparency and trust.	Although the specification concentrates on security, it seems to be possible to extend it to monitor and to validate a broader range of service level and service quality objectives.

2.2.2.4 Cloud Interoperability and Federation

Table 5: Standards related to Cloud Interoperability and Federation

Standard	SDO	Summary	Relevance
Open Cloud Computing Interface (OCCI) [34]	OGF	OCCI is a Protocol and API for all kinds of management tasks with a strong focus on integration, portability, interoperability and innovation while offering a high degree of extensibility	Most influential standard for the creation and management of interoperable and federated cloud services supported by a large variety of implementations.
Cloud Application Management for Platforms (CAMP) [35]	OASIS	CAMP provides a common basis for developing multi-cloud management tools as well as offering cloud providers and consumers a REST-based approach to application management. CAMP advances an interoperable protocol that cloud implementers can use to package and deploy their applications. It provides a common development vocabulary and API that can work across multiple clouds without excessive adaptation and is compatible with PaaS-aware and PaaS-unaware application development environments, both offline and in the cloud.	As with [34], these standards provide several approaches to ensure interoperability and portability in distributed or federated cloud systems. Although they are not directly relevant for ACSmI since they are not dealing with SLAs, a general knowledge on how interoperability and portability can be implemented in a cloud system is needed to ensure a consistent approach within the project.
Cloud Infrastructure Management Interface (CIMI) [36]	DMTF	This specification standardizes interactions between cloud environments to achieve interoperable cloud infrastructure management between service providers and their consumers	

Standard	SDO	Summary	Relevance
		and developers, enabling users to manage their cloud infrastructure use easily and without complexity.	
Topology and Orchestration Specification for Cloud Applications (TOSCA) [37]	OASIS	The standard enhances the portability of cloud applications and services providing a machine-readable language to describe the relationships between components, requirements, and capabilities. TOSCA enables the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behaviour of these services.	
Cloud Data Management Interface (CDMI) [38]	SNIA	The standard defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud. As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface.	

2.3 Legislation

2.3.1 ACSmI alignment with legislation

The Advanced Cloud Service meta-Intermediator (ACSmI) has to be aligned with applicable legislation. This of course means that the ACSmI itself as a tool should be compliant with legislation, but what also should be considered is the compliance of the services ACSmI aims to play a brokering role in.

As far as ACSmI itself is concerned, compliance issues would foreseeably relate to contractual aspects, relating to the relation between the ACSmI user and the exploiting consortium partners, i.e. the business exploitation plan and the applicable terms and conditions. It should be noted that ACSmI could either function as a mere facilitator of direct contractual relations between the user and the CSP or ACSmI could directly contract services with the CSP, then redistributing them to the users. This could take the form of ACSmI being exploited through a specific legal vehicle. Most concerns relating to the terms and conditions of the use of ACSmI can be addressed at a later stage, when the project had matured. Those aspects that are of concern already at this stage will be addressed below.

What is of real importance at this stage is the legal compliance status of the services within ACSmI during the actual service operation and the function of ACSmI in this respect. Legal compliance can relate to contractual aspects such as conclusion and termination of contracts, data location, data protection, data portability, interoperability or rules blocking the free flow of non-personal data etc. While many of these aspects might not directly affect the functioning of the service, they may be very relevant for the user of the service. Therefore, they should be considered prior to the selection and launch of the specific set of cloud services used for a particular application as NFRs on the application level and ACSmI should show their fulfilment, playing a facilitating role for the selection by the cloud user of the services that fit both the functional requirements of the envisioned processing or application and the legal requirements/preferences of his or her organization.

For example, processing sensitive health information might have to deal with national laws requiring the data to be stored within the territory of the jurisdiction concerned. Such an application will have to comply with data protection legislation, namely the GDPR [39], and the rules on data portability and interoperability such legislation contains, forcing the application to have built in privacy features by design and default. Moreover, for the AIMES use case the effects of Brexit will have to be taken into account. Equally, the use of ACSmI to have an application run on multiple clouds (whether or not through the use of services from multiple cloud providers) will have to be contractually sound, enabling the user to check whether the different SLA's of the composed services are clear and compatible, so that the multi-cloud SLA (MCSLA) is enforceable and logically consistent.

While ACSmI should facilitate the accomplishment of legal compliance as much as possible, it does not take any legal responsibility itself. This should be especially clarified if the option is chose to have ACSmI directly contract services with CSPs. ACSmI is a tool aimed at stimulating the discovery, negotiation and contracting of the most suited cloud services for a given application. Its goal is to help identify and contract the specific set of cloud services for an application that fulfils the technical/functional requirements as well as the legal and other NFRs. While the ACSmI should strive to ensure that the information is as accurate as possible, it should deny any liability on this part. It is the cloud provider who is responsible for providing the correct information on their service. ACSmI should do nothing more than aggregate, combine and transfer this information. From a contractual point of view the situation depends on the option taken. If ACSmI does not directly contract services, the cloud user would then directly enter into a contract with the cloud service provider, in the full knowledge that the information provided to him via ACSmI reflects the up-to-date and only commitment on the part of the CSP, with ACSmI taking no legal responsibility in the brokering of the contract. If ACSmI does directly contract services with the CSP, the same result should be obtained.

In any case, the legal relation between the user and ACSmI, that is the term and conditions of the use of ACSmI should clearly provide that there is a reasonable effort obligation at most.

Equally, under data protection law, the cloud user will retain responsibility in both scenarios. The cloud user will typically be considered as the data controller, who has assigned obligations under the applicable law. Those obligations cannot be transferred, except to the processor through explicit contractual arrangements and to a limited extent, as permitted by the relevant law. The CSP will typically be qualified as a data processor in a scenario such as present in the DECIDE framework. Contractual arrangements between the CSP/data processor and the user/data controller are recommendable, and ACSmI could play a role in clarifying to what extent the CSP commits itself to certain arrangements. The relation between ACSmI, the CSP and the user should be clearly defined in terms of data protection obligations as well. However, the principle remains that both data controller and data processor have their respective obligations under the applicable data protection law, as a result of the function they perform in the processing of personal data. Therefore, compliance with controller obligations imposed by applicable law remains with the cloud user/data controller. Examples include the right of the data subject to data portability, the right to object and the right to erasure.

Lastly, other potential legal obstacles should be considered, e.g. those national rules obstructing the free movement of non-personal data in the EU, which could equally prevent the use of a service from CSP in Member State X by a user in Member State Y. The result should again be that ACSmI's responsibility is interpreted as narrowly as possible. The CSP has to flag the potentially problematic rules they are aware of in relation to the service offered. The user of the cloud service from his or her side has to properly inform him- or herself of the relevant law applicable to the intended processing, based on the information provided by the CSP. ACSmI essentially acts as a mere conduit tool, facilitating the discovery of services, aiding negotiation and providing efficient contracting possibilities. The effect should in essence be the same even in case where ACSmI would directly contracts services from CSPs. It remains a mere facilitation of finding and using the right set of cloud services. ACSmI should not be held to perform a controlling role. The terms and conditions will have to clarify this.

In conclusion, there are no clear issues with the ACSmI being aligned with applicable legislation. As far as legal issues of the services endorsed within ACSmI are concerned, ACSmI can play a role in flagging these issues by encouraging CSP's to provide sufficient information, thus enabling a fully informed assessment by the user. Nonetheless, ACSmI should bear no responsibility of its own, neither contractually or otherwise.

3 Main actors of the ACSmI

The following is the list of actors involved in ACSmI, which is aligned with the actors defined in D2.1 [1]

- **DECIDE operator:** the DECIDE operator fulfils tasks that correspond to both a developer and an operator. In the traditional sense, the developer develops the offer that was presented by the responsible of the acquisition project, as well as new functionalities that arise during development, based on the technologies that the client demanded. On the other hand, the operator is in charge of ensuring the proper working of the application. However, DECIDE fosters a DevOps approach, so the distinction between these two actors gets blurred. The DECIDE operator takes on developer's responsibilities before deployment and operator's responsibilities after deployment.

- **Cloud Services Provider:** company that offers network services, infrastructure or business applications in the cloud. These cloud services are hosted in the company's data centers and are accessible to users through the Internet.

In the context of the ACSmI, these actors can perform different activities depending on the role they play. At this stage of the project we envision the following roles for ACSmI:

- Multi-cloud application operator,
- Multi-cloud application owner,
- ACSmI administrator,
- ACSmI operator including a law expert, accountability department, and so on,
- CSP

4 General Description of the Solution

4.1 Main objectives of the ACSmI

The Advanced Cloud Service (meta-) intermediator (ACSmI) will provide means to assess continuous real time verification of the cloud services non-functional properties fulfilment and legislation compliance enforcement. ACSmI will also provide a cloud services store where developers can easily access centrally negotiated deals of compliant and accredited and applications developed by the software sector.

In the following use case diagram, the main functionalities of the ACSmI are detailed.

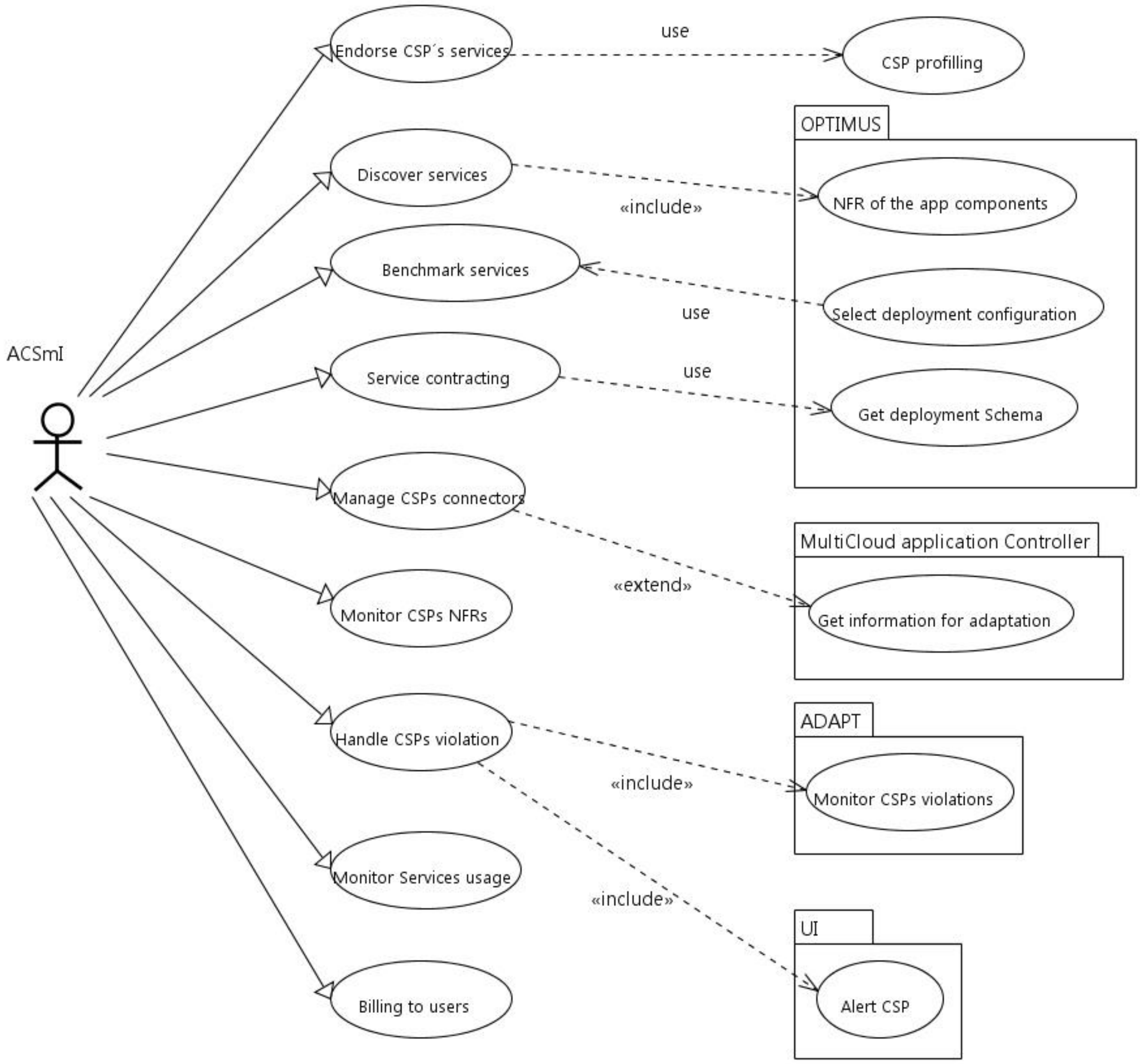

Figure 1: Main functionalities of ACSmI

There are six main functionalities envisioned:

1. Endorse a cloud service into the ACSmI. ACSmI will allow to registry services. This can be done by the CSP, by the multi-cloud application operator or by the ACSmI Administrator. The registry of each service should cover the different defined terms for modelling the CSPs and their services. This will allow the discovery of the services from the services registry.

2. Discover and benchmark services. OPTIMUS will indicate the NFR of the services that shall be delivered to the ACSmI as input. ACSmI will discover, from the services stored in its registry, the most appropriate ones for that set of NFRs. Then, from the set of discovered services, ACSmI will prioritize these services in terms of NFRs fulfilment (including legal aspects) which will be passed to OPTIMUS a short list. The short list will include, additionally, the degree of fulfilment of the NFRs requested by the user.
3. Contract services. This functionality will allow dealing with all the activities related to the contracts with the ACSmI. Depending on the type of services and the CSP, ACSmI will manage the contract in two different ways: 1) ACSmI will facilitate contracting services directly by the user to the provider and 2) ACSmI will manage the contract itself with the provider and the user. In this case, ACSmI will have mainly two types of contracts. The first one is the contract with the CSP and the other one is with the user of the services intermediated by the ACSmI.
4. Manage CSPs. This functionality will allow the management of the different connectors to facilitate the contracting of the services and to monitor them. This functionality will be in charge of informing ADAPT with the required information for the deployment of the multi-cloud application through the different contracted services.
5. Monitor NFR CSPs and manage the violation alerts. This functionality will monitor the SLA (NFRs) of the service offered by the CSPs to detect any violation of the SLAs during the operation of the services. If a violation is detected, an alert to ADAPT will be sent.
6. Monitor the use and bill the user. This functionality will allow calculating the costs made by the user for the use of the ACSmI services, ant to provide the corresponding receipt. To be able to generate the billing of the contracted services, the ACSmI shall monitor the use of the different cloud services.

4.2 High level architecture

The high level architecture of the ACSmI is presented next.

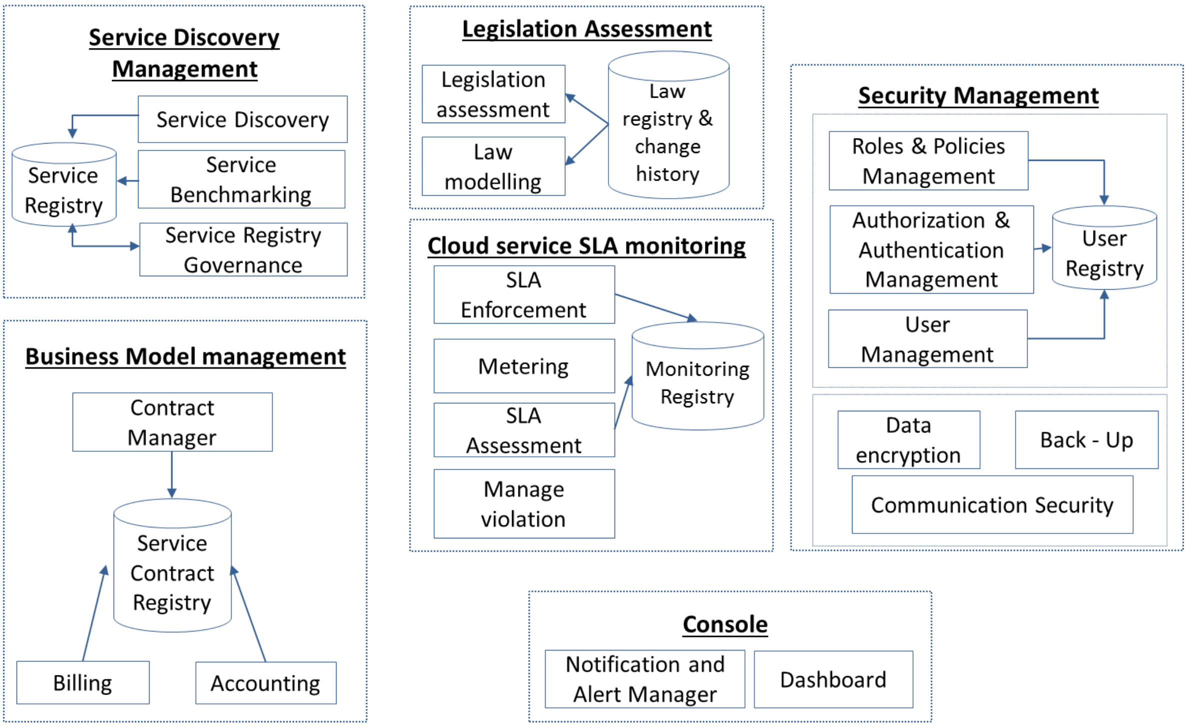

Figure 2: ACSmI High Level Architecture

There are six main components in charge of implementing the core functions of the ACSmI. Here a high level description of the main components and their corresponding sub-components is presented.

1. **Service Discovery Management**: This component is in charge of executing and managing all the operations related to the services offered by the ACSmI. Functions like cloud services endorsement, intelligent discovery, or service operation are covered by this component and the corresponding sub-components. The sub-modules included in the Service Management are:
   a. ***Service Registry***: The service registry is in charge of registering all the information related to the services offered by the ACSmI. The type of information to be registered will be related to the information about the NFRs.
   b. ***Service Registry Governance***: The Service Registry Governance is responsible for managing the access and update to the service registry.
   c. ***Discovery Service***: This sub-component is in charge of managing the requests from the users (OPTIMUS) to discover the services. It gathers and processes the NFRs from OPTIMUS when discovering services in the ACSmI.
   d. ***Benchmarking of the services***: This sub-component will be in charge of comparing the different NFRs of the services and providing a short list of services based on the degree of the fulfilment of the NFRs

2. **Legislation Assessment:** The legislation Assessment is in charge of assessing the compliance of the services with respect to the different legislations (i.e. GPDR and Code of Conduct of CSPs). The sub-modules included in this module are:
   a. ***Regulations Compliance Assessment:*** This is the sub-module which manages the core functions with respect to legislation assessment. It assesses the different services with respect to the legislation included in the Law registry of the ACSmI.
   b. ***Law Registry:*** It stores the information of the different legislations to be considered in the ACSmI.
   c. ***Regulations Change History:*** This registry stores the changes suffered by the different legislations (i.e. updates, new versions, etc.).
   d. ***Law Modelling:*** It allows the legal experts to model the different legislations so that the legislations assessment can be done in the ACSmI.

3. **Cloud service SLA monitoring:** This module is in charge of the management of the monitoring of the services in the ACSmI. This module is composed of the different sub-modules to perform the corresponding activities:
   a. ***SLA Enforcement:*** It is in charge of monitoring the SLAs.
   b. ***SLA Assessment:*** It assesses the compliance of the SLA of the service
   c. ***Metering:*** It measures, according to the established metering mechanism, the metrics defined in the SLA and returns the values of these metrics.
   d. ***Manage violation.*** This sub module is in charge of managing and alert that a service in the ACSmI is not fulfilling the SLA.

4. **Business Model management:** This core component is in charge of the execution and management of all the operations related to Service Contracts in the ACSmI. It also performs all the activities related to the financial operations with the different users of the ACSmI The sub-modules included in this component are:
   a. ***Contract Manager:*** It is in charge of the management the core functions with respect to the service contracts. It manages mainly two different types of contracts: The contracts between the user and the ACSmI and the contracts between the CSPs (service providers) and the ACSmI.

b. ***Service Contract Registry:*** This sub-module stores the different contracts existing in the ACSmI.
c. **Accounting:** It is responsible for monitoring and calculating the total values in order to bill the users for the services and to pay the CSPs for the services used.
d. **Billing:** It generates the bills for the users.

5. **Security management**: This component is in charge of designing and developing the means to guarantee the secure operation of the ACSmI including identity propagation and federated authentication and authorization, but not only, as this module deals with all the aspects related to the management of security of the ACSmI, such as data and communication security as well as backup services. These services shall secure all data generated and stored resulting from the activities performed by the ACSmIitself. These shall be stored in the service registry, service contract registry and user registry components of the ACSmI. The sub-modules included in this component are:
    a. ***Roles Manager***: It manages the activities related to the roles in the ACSmI (creation, modification, assignment, deletion).
    b. ***Policy Manager***: It manages the activities related to the policies in the ACSmI (creation, modification, assignment, deletion).
    c. ***User Manager***: It manages the activities related to the users in the ACSmI (creation, modification, roles assignment, deletion).
    d. ***User Registry***: It stores all the information associated to the users of the ACSmI.
    e. ***Authentication* Manager**: This sub-module performs the authentication of the users and manages the access to the different actions/functions of the ACSmI for every user.
    f. ***Communication Security***: It provides secure communication means using the SSL transport layer encryption both between the client and the platform as well as between the platform and cloud infrastructures.
    g. ***Backup service***: It is responsible to carry out incremental back-ups for allowing the recovery of data of the ACSmI in case it is necessary.
    h. ***Data encryption***: It is responsible to encrypt the data of the ACSmI in order to maintain secured these data in case of cyber-attacks.

6. **Console:** The Console is the module in charge of implementing the interface with the different users in the ACSmI. The sub-modules included in the Console are:
    a. ***Notification and Alert Manager:*** It manages the different alerts and notifications that are shown to the user.
    b. ***Dashboard:*** This is the user graphical interface. It will be customized depending on the type of user, role and the actions allowed by the corresponding policy.

5 ACSmI Requirements

In the following sections the initial elicitation of ACSmI requirements is presented.

5.1 CSPs service discovery and management

5.1.1 Functional requirements

Req. ID	DIS01
Req. Short Title	Endorse a cloud service into the ACSmI.
Req. Description	CSPs or the ACSmI administrator (for Large CSPs) register(s) one of its services or large CSP´s services in the service registry. The registry of each service shall cover the different terms defined in the modelling of the CSPs and their services. This will allow the discovery of the services from the registry.
Phase/sub-phase of the DevOps framework	Operation phase/Pre- deployment preparation
Supported Functionality of the DevOps framework	Create and update the service registry into the ACSmI
Source	DoA
Priority	High

Req. ID	DIS02
Req. Short Title	Specify a set of (non-)functional requirements in order to discover the services.
Req. Description	The (non-functional) requirements of the multi-cloud application shall be collected by OPTIMUS and passed to the ACSmI so that services from the service registry fulfilling such requirements can be discovered. The requirements will be specified following the different terms defined for the modelling of the CSPs and their services. This allows an automatic comparison of the requirements with the services stored in the registry.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud services discovery
Source	DoA
Priority	High

Req. ID	DIS03
Req. Short Title	Discovery of services
Req. Description	The objective is to provide a list of services from the services registry that fulfil (totally or partially) the requirements specified by the DECIDE operator. These requirements are specified in the DIS02.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud services discovery
Source	DoA
Priority	High

Req. ID	DIS04
Req. Short Title	Federated Discovery of services
Req. Description	The objective is to provide a list of services from other ACSmIs that fulfil (totally or partially) the requirements specified by the Cloud Consumer (multi-cloud application). These requirements are specified in the DIS01. Provide a list of services from another
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery
Source	DoA
Priority	Low

Req. ID	DIS05
Req. Short Title	Benchmark of services
Req. Description	The discovered services (DIS03, DIS04) shall be prioritized. Depending on the level of fulfilment of the NFRs expressed by the DECIDE operator, the discovered services will be sent back to DECIDE operator in the form of a sorted list, indicating the degree of fulfilment.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the	Cloud service discovery

DevOps framework	
Source	DoA
Priority	High

Req. ID	DIS06
Req. Short Title	User management.
Req. Description	The objective is to provide means to create, read, update and delete (CRUD) the users´ registry. When creating a new user, a role shall be assigned to him, and based on this role, the allowed activities to be performed shall be associated to this user. The different types of roles envisioned are: CSP, multi-cloud application operator, multi-cloud application owner, ACSmI administrator and ACSmI operator. This requirement is related to the Roles management (SEC01) and Security Policy management (SEC02).
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud services discovery/ Could services monitoring/ Cloud services contracting.
Source	DoA
Priority	High

Req. ID	DIS07
Req. Short Title	Service registry management
Req. Description	The objective is to provide means to create, read, update and delete the services registry. This registry shall record not only information provided by the CSPs, but also other information such as which multi-cloud application is using the service, SLAs violations, legal compliance and so on. The service registry management shall be aware of the alerts of potential SLA violations as well as non-legislation compliance (MON06 & LEG02) in order to update appropriately the registry.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery
Source	DoA
Priority	High

Req. ID	DIS08
Req. Short Title	Dashboard management
Req. Description	The objective is to handle the dashboard that shall be personalised depending on the role of the ACSmI users. ACSmI shall customise the dashboard to show users only the allowed tasks to be performed.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Dashboard management
Source	DoA
Priority	High

Req. ID	DIS09
Req. Short Title	Service withdrawal
Req. Description	The objective is to remove a service from the service registry so that it cannot be used any more in the discovery process. To remove a service from the registry, the multi cloud applications using those services have to be considered, in order to alert them of the withdrawal of the service and to provide them with an alternative solution.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation Operation phase/Application monitoring
Supported Functionality of the DevOps framework	Cloud service contracting CSP Monitoring
Source	DoA
Priority	Medium

5.2 Dynamic monitoring of CSPs SLAs

These requirements have the objective of monitoring and assessing that the aggregated and intermediated cloud offerings fulfil the corresponding SLA terms and conditions, including legislation and accreditation issues, security aspects and propagation of changes.

The main aim is to assess theoretical SLA and QoS (e.g. performance) values, as provided by the CSP with respect to the ones resulting from these monitoring activities. This information will be, on one hand, accessible to the users, but on the other, also internally as it will feed the SLA monitoring module in order to detect violations with respect to the agreed QoS.

5.2.1 Functional requirements

Req. ID	MON01
Req. Short Title	Define the firewall port (Standard open ports)
Req. Description	The objective is to define a default firewall policy to be established before every deployment to cover the needs of open and closed ports necessary to ensure the correct application running once deployed in the multi-cloud environment.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud service contracting
Source	Other
Priority	Medium

Req. ID	MON02
Req. Short Title	Define the monitoring method (Push or pull).
Req. Description	The objective is to offer the "push" and "pull" monitoring methods. • “Push Monitoring” means: Clean monitoring. No additional facilities or agents required. As it does not need additional software installation, the monitoring activities will not impact the performance. • “Pull Monitoring” means: Full monitoring. Depending on the technology used by the CSP, it shall be necessary to install different types of software / agents on the cloud server where the application is deployed. This method allows monitoring any aspect/parameter/process of both the application and the Cloud Server. It is more accurate than the Push Monitoring
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	CSP monitoring
Source	Other

Priority	Medium

Req. ID	MON03
Req. Short Title	Define the monitoring parameters
Req. Description	The objective of this requirement is to relate the different SLA terms and NFRs, to the parameters to be monitored by ACSmI. This shall generate a generic list of parameters to be monitored for each NFR and SLA term.
Phase/sub phase of the DevOps framework	Operation phase/ Application Monitoring
Supported Functionality of the DevOps framework	CSP monitoring
Source	Other
Priority	High

Req. ID	MON04
Req. Short Title	Manage the list of parameters to be monitored
Req. Description	Based on the SLA contracted and the NFRs, the list of parameters to be monitored shall be selected from the generic list of parameters (MON03)
Phase/sub phase of the DevOps framework	Operation phase/Application Monitoring
Supported Functionality of the DevOps framework	CSP monitoring
Source	DoA
Priority	High

Req. ID	MON05
Req. Short Title	Check MCSLA from the DECIDE DevpOps Framework
Req. Description	The objective is to gain access to the composite MCSLA created by the DECIDE DevOps framework in order to parse the parameters to be monitored.
Phase/sub phase of the DevOps framework	Operation/Application Monitoring

Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	MON06
Req. Short Title	Alert of an SLA violation
Req. Description	If a SLA parameter is violated, means to alert the operator (ADAPT) as well as the service user about which parameters have been violated in order to create a new deployment configuration shall be put in place. This shall ensure a more reliable service.
Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	MON07
Req. Short Title	Get monitored values for a given parameter
Req. Description	The objective of this requirement is to provide the ACSmI user with the current and historical values of the parameters that are being monitored according to the SLA terms.
Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	MON08
Req. Short Title	Assess the CSP´s SLA

Req. Description	A SLA Assessment has to take place as it provides insight on whether the CSPs will fulfil the SLA in its entirety or whether it needs to be re-evaluated, amended or undergo through changes.
Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	MON09
Req. Short Title	Get log of violations
Req. Description	All violations shall be logged and the log shall be obtainable by the users. The log shall hold the following parameters and values: • CSP Id/info • Violated parameters • Value of violated parameters • Time and date of parameters • Application id • Other data • The log should be read only, hashed and signed by ACSmI
Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	MON10
Req. Short Title	Define the monitoring parameters
Req. Description	The monitoring component of the ACSmI shall store all definitions on how to monitor the specified parameters in a machine-readable way
Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA

Priority	High

5.3 Security management

This section is in charge of the design and development of the means to guarantee the secure operation of the ACSmI, including identity propagation and federated authentication and authorization.

5.3.1 Functional requirements

Req. ID	SEC01
Req. Short Title	Roles management
Req. Description	The objective is to provide means to create, delete and modify roles in the ACSmI to be assigned to the users (DIS06). The main roles envisioned are: CSP, multi-cloud application operator, multi-cloud application owner, ACSmI operator and ACSmI administrator.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud service Discovery Cloud service contracting CSP Monitoring
Source	DoA
Priority	High

Req. ID	SEC02
Req. Short Title	Security Policy management
Req. Description	The objective is to provide means to create, delete and modify policies in the ACSmI to be assigned to the roles. These policies are activities and rules that shall be accomplished by ACSmI.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery Cloud service contracting CSP Monitoring
Source	DoA
Priority	High

Req. ID	SEC03
Req. Short Title	Authentication & Authorization
Req. Description	The objective is to authenticate a user based on the user credentials as well as to provide access to allowed actions considering its role.
Phase/sub phase of the DevOps framework	Operation phase/ Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery Cloud service contracting CSP Monitoring
Source	DoA
Priority	High

Req. ID	SEC04
Req. Short Title	Communication layer security
Req. Description	Communication layer security using SSL transport layer encryption both between the client and the platform and between the platform and the cloud infrastructures.
Phase/sub phase of the DevOps framework	Operation phase/Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery Cloud service contracting CSP Monitoring
Source	DoA
Priority	High

Req. ID	SEC05
Req. Short Title	Data encryption
Req. Description	Users shall be able to store their data encrypted in a cloud storage service. This feature will be optional: a user can select either to encrypt the data stored or to leave them unencrypted.
Phase/sub phase of the DevOps framework	Operation phase/Pre-deployment
Supported Functionality of the DevOps framework	Cloud service Discovery Cloud service contracting CSP Monitoring
Source	DoA

Priority	High

Req. ID	SEC06
Req. Short Title	Secure API access in ACSmI
Req. Description	The objective of this requirement is to allow ACSmI users to setup the configuration for their account in the following way: all the items available under the particular user account (e.g. software, resources) will be reachable via API from predefined IPs only. For example, only users who access ACSmI from predefined IPs only can use particular resource via API. The feature is configurable: if a user would like to allow access from any other IP - it will be possible to do so; however, it will be possible to restrict the access as well.
Phase/sub phase of the DevOps framework	Operation phase/Pre-deployment
Supported Functionality of the DevOps framework	Cloud service discovery Cloud service contracting CSP Monitoring
Source	DoA
Priority	Medium

Req. ID	SEC07
Req. Short Title	Client data backup and archiving
Req. Description	This feature will allow to backup and archive ACSmI users´ data so that in case of need or emergency, they could be easily recovered. This will ensure ACSmI´s data integrity and safety.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	ACSmI set-up
Source	DoA
Priority	Low

Req. ID	SEC08
Req. Short Title	Implement specific security requirements for each use case
Req. Description	The objective is to implement the security requirement for particular use case. ACSmI should cover all the security aspects required by the use cases.

Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud services discovery
Source	Use cases
Priority	High

5.4 Legislation compliance and monitoring

5.4.1 Functional requirements

Req. ID	LEG01
Req. Short Title	Show legally relevant aspects when initiating a service
Req. Description	Show legally relevant aspects when initiating a service, in particular in regards to location of data, data security level, location of the service provider etc. in order to enable the cloud consumer to assess legal impact of initializing and operating the proposed service.
Phase/sub phase of the DevOps framework	Operation phase/Pre-Deployment
Supported Functionality of the DevOps framework	Cloud services discovery
Source	DoA
Priority	High

Req. ID	LEG02
Req. Short Title	Show the legal mechanisms when non-compliance of SLA
Req. Description	ACSmI should be able to indicate to the DECIDE operator which actions could be taken when the SLA associated to a service is not accomplished.
Phase/sub phase of the DevOps framework	Operation phase/deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	Medium

Req. ID	LEG03
Req. Short Title	Show contractual consequences of (automatic) redeployment
Req. Description	ACSmI shall show how contracts are terminated and concluded with another provider in case of redeployment of parts of the affected application.
Phase/sub phase of the DevOps framework	Operation phase/deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	LEG04
Req. Short Title	Show legally relevant aspects on exit
Req. Description	ACSmI shall be able to show what terms regulate the termination of a service, e.g. data format on exit, data portability, security measures etc.
Phase/sub phase of the DevOps framework	Operation phase/deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	Other
Priority	High

5.5 Business modelling implementation

The objective is to develop methods and tools that enable the control, monitoring and billing of the use of the services of the ACSmI.

This block is going to allow the contracting of the cloud services supporting the defined business model for ACSmI (WP7).

5.5.1 Functional requirements

Req. ID	BUS01
Req. Short Title	Monitor and control the service status.
Req. Description	The objective is to check the service status via the ACSmI (e.g. if the service is operational or not).

Phase/sub phase of the DevOps framework	Operation/Application Monitoring
Supported Functionality of the DevOps framework	CSP Monitoring
Source	DoA
Priority	High

Req. ID	BUS02
Req. Short Title	Implement the procedures to get access to a service
Req. Description	The objective is to implement the features that facilitate the multi-cloud application operator to get access to the service. ACSmI shall provide the multi-cloud application operator with details of how the access can be obtained. It is (often) impossible to get instant access to some resources. The CSP may request detailed information from the multi-cloud application operator. After the CSP checks the information and decides that the multi-cloud application operator can be allowed to the service, the multi-cloud application operator gets appropriate access. An example of such provider is HLRS (High-Performance Computing Center in Stuttgart [40]): HLRS provides extremely powerful infrastructure for its users, however, requires a specific procedure to be completed before getting a cloud account.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Application Monitoring
Source	Operation phase/Deployment preparation
Priority	Cloud services contracting

Req. ID	BUS03
Req. Short Title	Charge a user in the background for service usage.
Req. Description	Each user shall be charged for service usage if there are specific prices for this service. To ensure this, a reasonable billing mechanism shall be available. It shall be possible to charge user in a background while the service is being used.
Phase/sub phase of the DevOps	Operation phase/Deployment preparation

framework	
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS04
Req. Short Title	Provide a user with usage reports.
Req. Description	Since the user is charged on actual service consumption basis, detailed reports related to the resources consumed shall be provided to the user. A user shall be able to see how many services and when they have been used.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS05
Req. Short Title	Provide a user with periodical invoices.
Req. Description	The objective is to enable a regular invoicing. Since a user is charged for service consumption, it would be very convenient to bill the user on periodical basis. It shall allow the user to get an official billing document as well as ACSmI and CSPs to get the user payments regularly.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS06

Req. Short Title	Provide a user with billing details.
Req. Description	Since the user is charged on actual resource consumption basis, it is important to provide a user with detailed reports related to the resources consumed and costs related to this consumption. A user should be able to see how much money, why and when he or she spent. It shall be possible to see estimated prices for different operations, as well as the casts produced.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS07
Req. Short Title	Contract a cloud service in the ACSmI
Req. Description	This requirement shall allow contracting a service or services in the ACSmI for a certain multi-cloud application owner. And ACSmI when receives the contract from the multi-cloud application owner, it contracts this service to the proper CSP.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS08
Req. Short Title	Contract a service directly with the CSP
Req. Description	This requirement shall allow developer to contract a service or services directly with the CSP. ACSmI will require the information for the contracted services (SLAs) to be included in the registry and to be monitored.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation

Supported Functionality of the DevOps framework	Cloud services contracting
Source	DoA
Priority	High

Req. ID	BUS09
Req. Short Title	Manage connectors
Req. Description	This requirement shall generate the APIs required to contract the services and monitor them in different CSPs. This requirement is closely related to the BUS02 requirement.
Phase/sub phase of the DevOps framework	Operation phase/Deployment preparation
Supported Functionality of the DevOps framework	Cloud service contracting Cloud service monitoring
Source	DoA
Priority	High

5.6 Non Functional requirements

The following requirements are based on the KPIs of the project related to this KR.

Req. ID	NF01
Req. Short Title	ACSmI must be functional
Req. Description	95% of functional requirements to be validated in each version are functioning well (with no errors). Functional test cases.

Req. ID	NF02
Req. Short Title	70% functionalities of ACSmI validated by the use cases
Req. Description	70% of the functionalities are validated by the use cases. Percentage of functional requirements for ACSmI implemented in the use cases.

Req. ID	NF03
Req. Short Title	Satisfaction by users 90%
Req. Description	Satisfaction questionnaires for the use cases, with rates of satisfaction of 90% or more.

6 ACSmI Design

In this section, the first version of the technical design of the ACSmI components is shown. The same structure has been followed for the description of each of the components. Firstly, the main functionalities of the component are described while secondly the component diagram is presented. In the component diagrams the Colour codes indicate the following:

- Yellow: components of the ACSmI that are outside of the described module
- Grey: components of the described module
- Red: other tools of DECIDE framework

6.1 CSPs service discovery and management

6.1.1 Main functionalities

The goal of the CSPs service discovery and management component (in the figures 'Service Management' for simplification issues) is to support the registering and the discovery of the services in the ACSmI service registry. The service registry of the CSPs service discovery and management component will take care of the creation, retrieval, update and delete operations of the services managed by the ACSmI. Deleting a service from a registry means the withdrawal of the service as well as the accompanying actions to perform this deletion in an appropriate way (e.g. archiving the data, warning other multi-cloud application providers using that service, and so on). The discovery and benchmarking components will respond to the requests of the non-functional requirements as provided by OPTIMUS or by the user of the ACSmI. Taking these requirements as input, the ACsmI will discover and benchmark the services that match these requirements. In summary, the main functional areas covered by the service management component are the following ones:

- Service registry
- Service withdrawal
- Intelligent service discovery

6.1.2 Component Diagram

To carry out the main functionalities described beforehand, this component needs to communicate with different modules of the ACSmI such as the Business Model Management and Dynamic monitoring of CSPs SLAs as well as also with other tools integrated in the DECIDE Framework such as OPTIMUS and ADAPT.

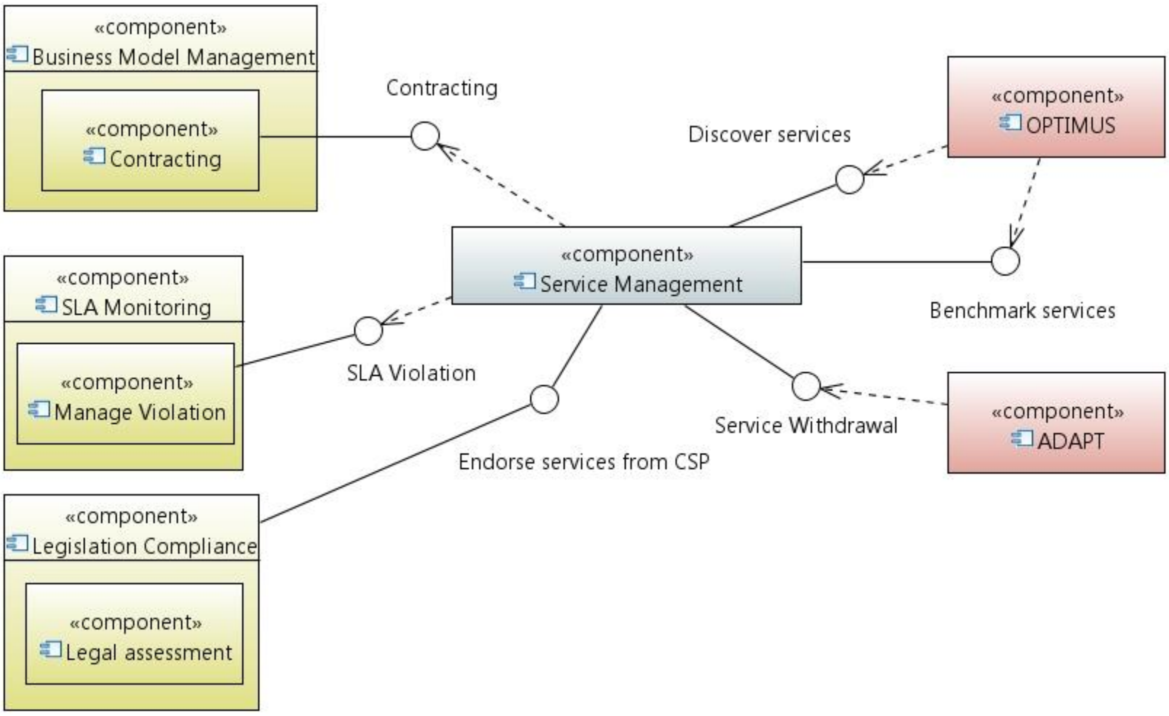

Figure 3: Service Management external component diagram

The CSPs Service Discovery and Management Component consists of five related sub-components, depicted in the next figure and described next:

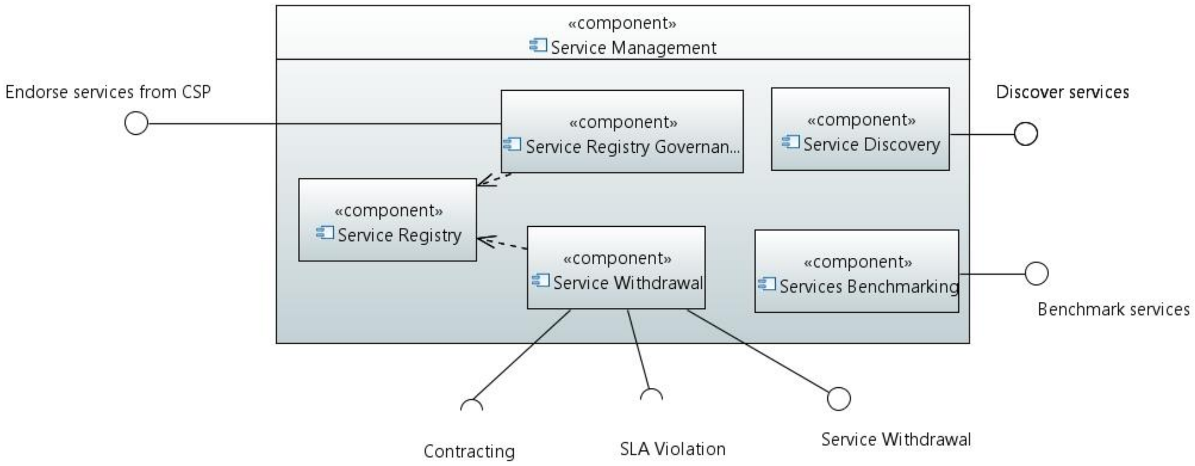

Figure 4: Service Discovery Management internal component diagram

- ***Service Registry***. This component is in charge of the registry of the services and their characteristics, such as the SLA, the regulatory compliance, their price, etc. This is a critical component as it is required in many processes.
- ***Service Registry Governance***, is in charge of the governance of the services. It shall take care of the different actions to be performed when a service is introduced or when a service is retired from the ACSmI service registry.
- ***Service Discovery***, supports the search for services. The input for these searches can be from two sources:

  - In the case in which the ACSmI is used as part of the complete DECIDE DevOps framework, the input will be provided by OPTIMUS, who needs this information to carry out the simulation before the deployment actually takes place.
  - In the case the ACSmI is used as a stand-alone tool and not integrated in the DECIDE framework, it is the user directly the stakeholder that shall provide with the information of the services to carry out the discovery.

- ***Service Benchmarking***, supports the comparison of different characteristics of the services in order to sort the discovered services according to the level of compliance of the NFRs.
- ***Service Withdrawal***, supports the deletion of a service from the service registry so it cannot be used any more in the discovery process. The decision of removing the service from the service registry can come from the ACSmI itself (e.g. repeatedly SLA violation), or from the CSP (e.g. business decision). This sub-component shall take into account that before withdrawing a service from the service registry it is necessary to analyse whether the service to be deleted is in operation and /or in use by any multi-cloud application from the service contract registry sub-module.

6.2 Dynamic monitoring of CSPs SLAs

6.2.1 Main functionalities

The goal of the Dynamic Monitoring of CSPs SLAs component (from now on ‘SLA monitoring’ for simplification issues) is to manage the SLA monitoring of the services included in the ACSmI. This encompasses the monitoring of the SLAs, which includes assessing the compliance of the SLAs of the services used, measuring the metrics defined in the SLA as well as alerting when a SLA term is violated.

6.2.2 Component Diagram

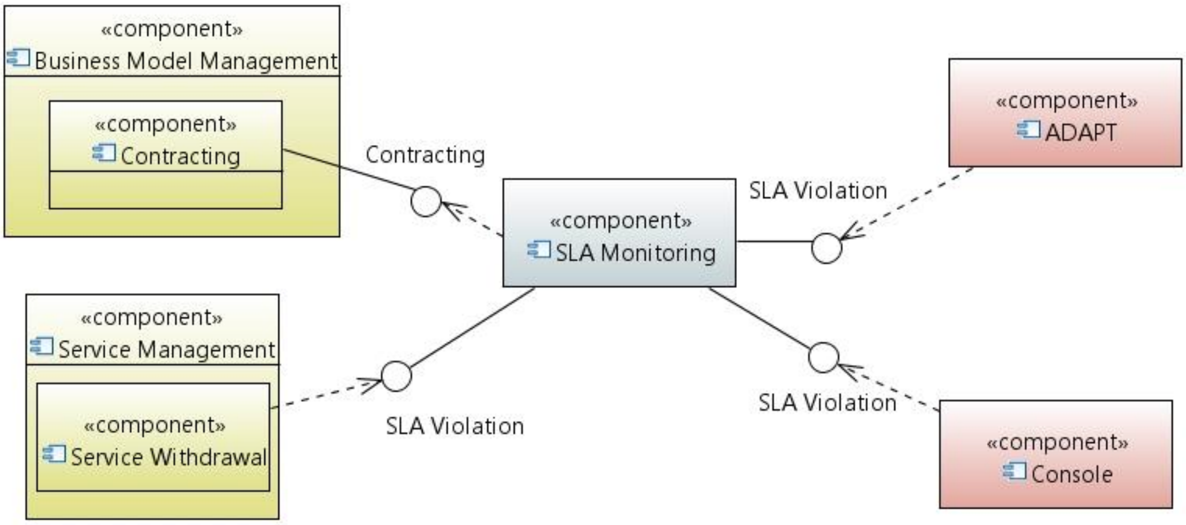

Figure 5: SLA Monitoring External component diagram

Figure 5depicts the SLA Monitoring component in relation to other components of ACSmI (yellow) and the DECIDE framework (red). The SLA Monitoring component interacts with the Business Model Management component in order to receive the contracted SLAs and parse the SLA terms to theparameters to be monitored. The interface to the component CSPs Service Discovery and Management ensures that violated SLAs are reported by the SLA monitoring component to facilitate the service withdrawal when required.

SLA violations are subsequently reported to the DECIDE Console in order to visualize them. Furthermore, ADAPT and the SLA Monitoring component will exchange metrics information.

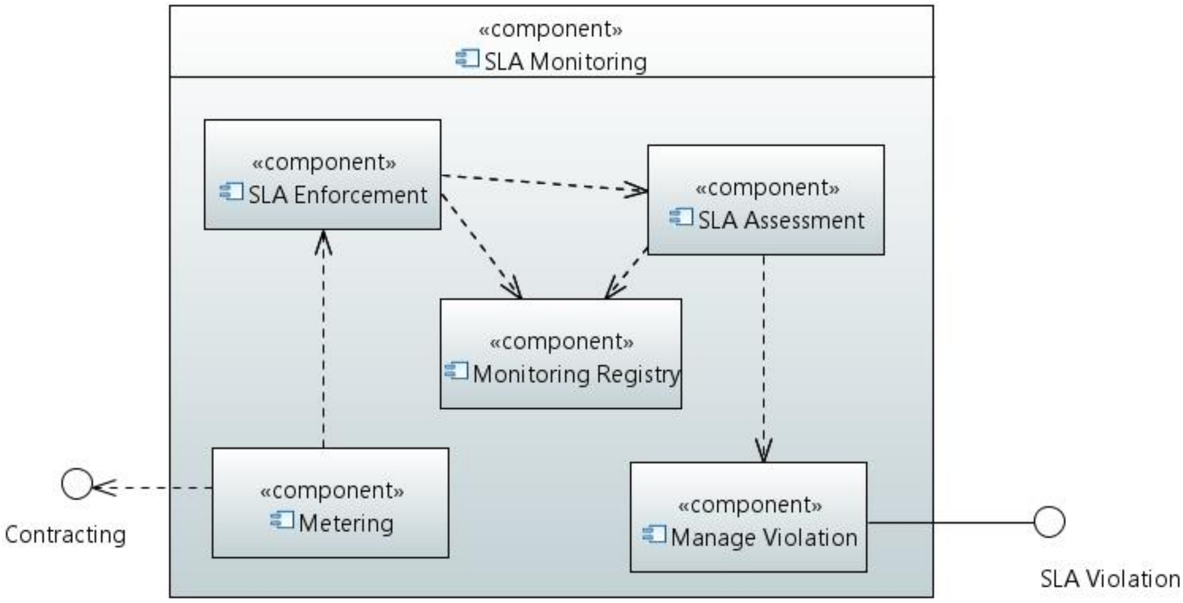

Figure 6: SLA Monitoring Internal component diagram

The SLA Monitoring component, which is in charge of monitoring the CSPs SLAs consists of 5 sub-components that collectively carry out this task. The sub-components are as follows:

- **Metering** collects the different SLA terms that will be monitored and selects the metric/parameters associated to each of the different terms. This module will use the 'Contracting' interface to receive the SLA terms that need to be monitored in a machine-readable way.
- **SLA Enforcement** retrieves the values of these parameters, and stores them in the monitoring repository.
- **SLA Assessment** assesses the compliance of the SLA of the contracted services with respect to the values retrieved for the parameters by the SLA enforcement sub-module (contracted values vs. real values).
- **Manage Violation** is a sub-module in charge of managing and triggering alerts when a service contracted by ACSmI is not fulfilling its SLA.
- **Monitoring repository** provides, assists, and automates the storage of metrics and values, and the detected violations in its repository

6.3 Security management

6.3.1 Main functionalities

This component has two main goals:

- To deal with all the activities related to the user management of the ACSmI, taken into account that there are four main roles: 1) Multi-cloud application operator, 2) multi-cloud application owner ; 3) Cloud services providers (CSPs) and 4) ACSmI administrator (including law experts, accountability department and so on). Another functionality of this module is the management of the policies and roles as well as the authentication management. If ACSmI is used integrated in the DECIDE framework, this functionality will be centralised for the whole framework. In case the ACSmI is used as a stand-alone tool, these functionalities shall be taken care by this component. Each user of the ACSmI shall have a role or policy assigned. Based on this role, ACSmI shall allow performing different actions. Moreover, in addition to this, the console for each user will be customised once the authentication management checks the validation of the credentials and based on his/her assigned role and allowed actions.

- To deal with all the aspects related to the management of the integrity of the ACSmI´s data. The data integrity in the ACSmI shall be focused on the data encryption, backup services and secure communications.

6.3.2 Component Diagram

To carry out these objectives, the Security Management component needs to communicate with several modules in the ACSmI such as the Service Registry, the User Registry and the Contract Registry components with the aim of allowing the securitization and backup of the data stored in these registries. Moreover, this component communicates with the Console component in order to obtain all the required information about the users, the policies and roles.

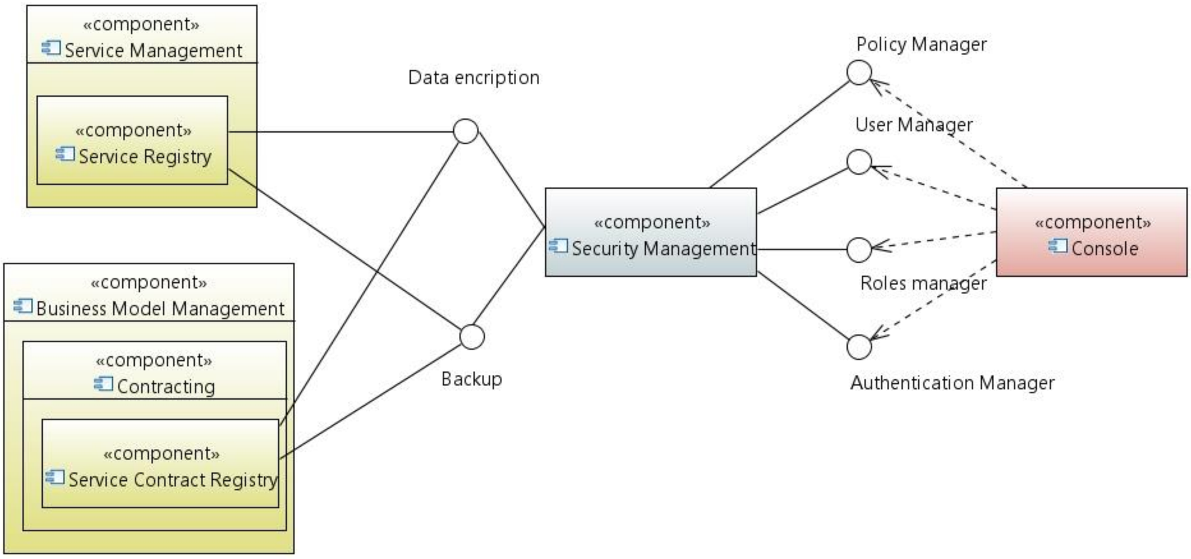

Figure 7: Security Management external component diagram

The Security Management component consists of eight related sub-components, which deal with the creation and management of users, the roles and the policies, and manage the issues to provide a secure ACSmI.

- ***User management*** is responsible for gathering the needed information to create, delete and modify users.
- ***Role Manager*** aims to create, delete and modify the roles of the ACSmI. Whenever a new user is created, the Role Manager sub-module is responsible to assign the role to this user. This component will update the user registry accordingly.
- ***Policy Manager*** aims to create, delete and modify the policies of the ACSmI. Whenever a new role is created, the Policy Manager sub-component is the responsible one to assign the policies that apply to this new role as well as to update the user registry accordingly.

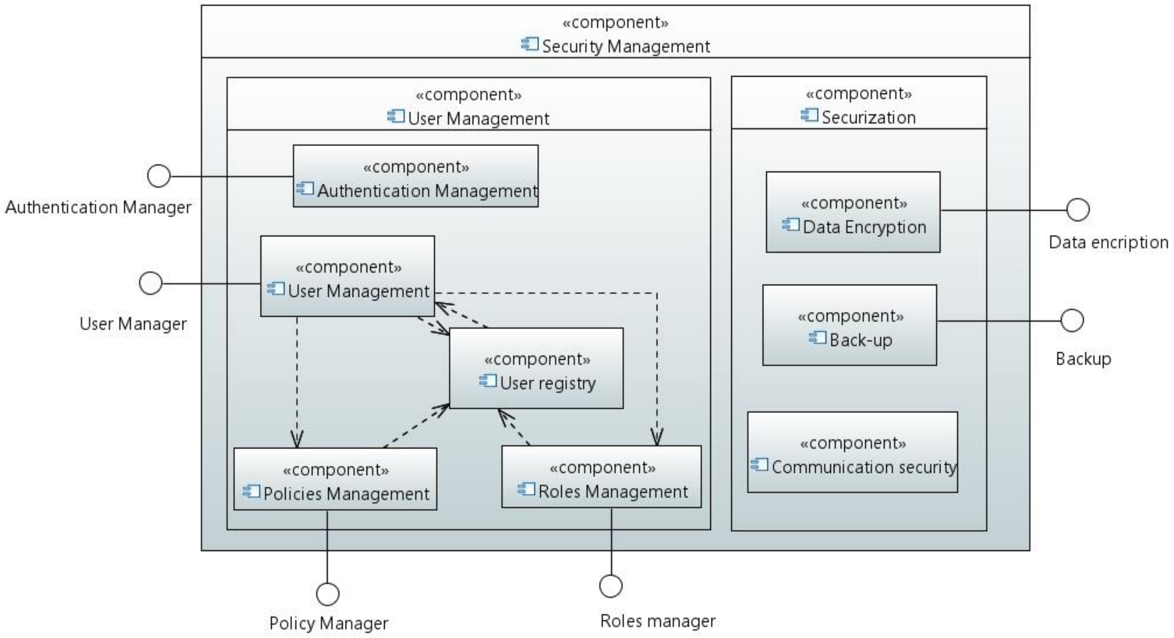
«component» Security Management
«component» User Management
«component» Authentication Management
«component» User Management
«component» User registry
«component» Policies Management
«component» Roles Management
«component» Securization
«component» Data Encryption
«component» Back-up
«component» Communication security
Authentication Manager
User Manager
Data encription
Backup
Policy Manager
Roles manager

Figure 8: Security Management internal component diagram

- ***Authentication Manager,*** is responsible for the authentication of the ACSmI users. In the case the ACSmI is integrated in the DECIDE framework, this component is not relevant. On the contrary case, if the credentials are valid, the authentication manager will provide the console with the identification token that will be used to propagate the identity to the rest of the modules when appropriate.
- ***User Registry*** is a database where all the information related to the users is stored.
- ***Data Encryption*** is responsible for the encryption of the ACSmI data so as to be able to maintain these data secure in case of cyber-attacks.
- ***Back- up*** is responsible for the execution of incremental back-ups that will allow the recovery of the ACSmI data in case it is necessary.
- ***Communication security*** is responsible for the provisioning of secure communications using the SSL transport layer encryption both between the client and the platform and between the platform and the cloud infrastructure.

6.4 Legislation compliance and monitoring

6.4.1 Main functionalities

This component (from now on, ‘Legislation compliance’) has two main goals:

- To provide means to assess the compliance of the services in the registry with respect to the data protection legislation [39]. This will be achieved by collecting legally relevant information whenever a service is endorsed in the registry, in particular in regards to the data localization, data security level, location of the service provider as well as location the data centre(s), data retrieval provision, data portability, liability caps, exit clauses, certification etc.
- To deal with all the legal aspects related to the contract (SLA) and the withdrawal of the service from the service registry. ACSmI shall have the contract stored in a machine readable format in order to be able to automate these steps.

6.4.2 Component Diagram

To carry out the first objective, the legislation compliance component needs to communicate mostly with the module Service Registry Governance with the main aim of obtaining the required data on the legal aspects of the service in question. The second objective requires knowing not only the SLA contracts but also the reasoning for the withdrawal. To achieve this, the module Legislation compliance needs to communicate with the modules Service withdrawal (part of Service Management component) and Contracting (part of Business Model Management component).

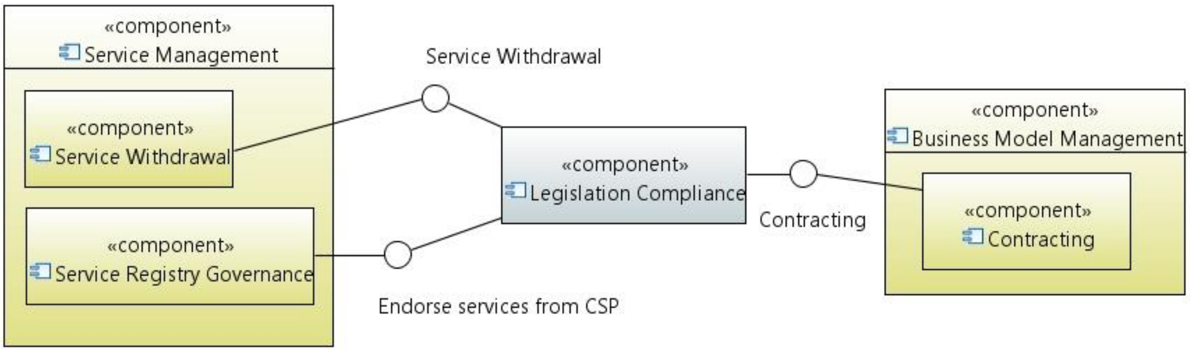

Figure 9: Legislation compliance external component diagram

The Legacy Compliance component consists of for related sub-components:

- ***Legal aspects component*** is a database where all the legal-related information gathered from the CSPs when endorsing a service is stored.
- ***Legal assessment component,*** is responsible of checking if the information collected from the CSPs accomplishes the requirements set by the applicable legislation, as requested by the user when eliciting the NFR. This module is also in charge of ensuring that any changes in the legislation will be propagated and all the services of the service registry will be reassessed.
- ***Enforcement of SLAs component***, is responsible of indicating what action is possible/ will be taken when one or more SLAs are not respected.
- ***Regulation of a service withdrawal*** is responsible of showing how contracts are terminated as well as what terms regulate the termination of a service, e.g. data format on exit, data portability, security measures etc.

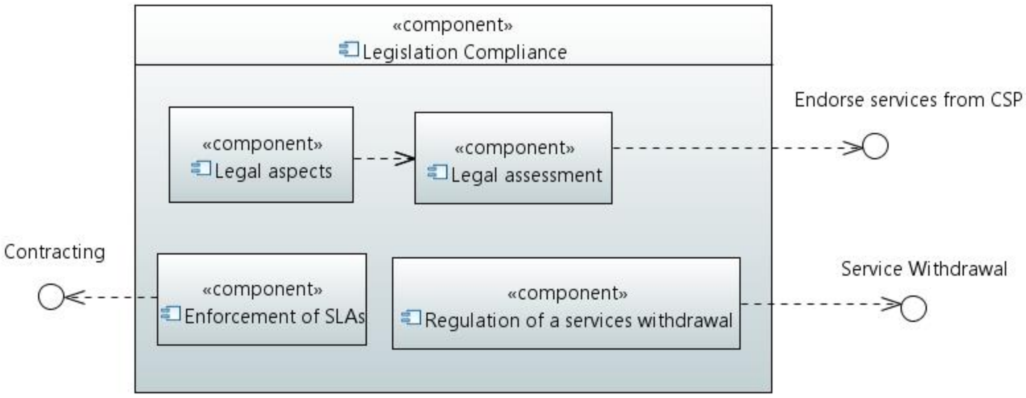

Figure 10: Legislation Compliance internal component diagram

6.5 Business modelling implementation

6.5.1 Main functionalities

The main objective of the Business Model Management component is to enable the implementation of the business model and related negotiated services. It shall also provide means for the contracting of services. To achieve these objectives, the following sub-components are envisioned under "Business Model Management" component:

- Billing component, that consists of Charging, Reporting Usage Data and Service and Price data sub-components.
- Contracting component.
- Data Accessor component.

6.5.2 Component Diagram

The Business Model Management component needs to connect to other ACSmI components in order to achieve its objectives. As it is shown in the figure below, the User Management component is required to deliver user data to the Billing sub-component of the Business Model Management component. The Metering component is required to provide service data for the Billing sub-component of the Business Model Management. Finally, ADAPT, Application Controller and Console components are required to interact with Data Accessor, Contracting and Billing components correspondingly. Please see the figure below for details.

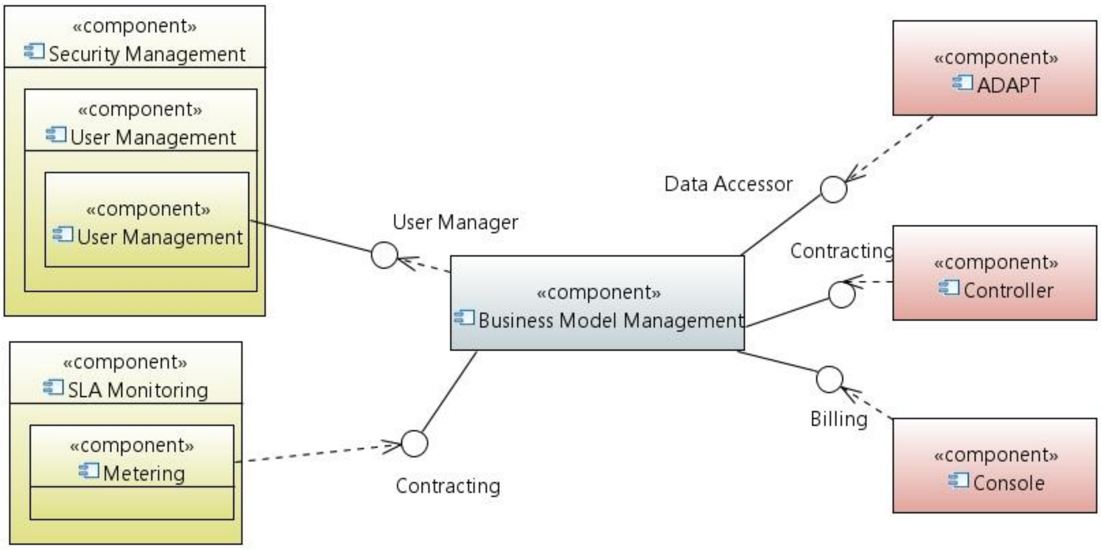

Figure 11: Business Model Management external component diagram

The Business Model Management component consists of 13 related sub-components that deal with the user billing, balance usage reporting, service contracting and data portability.

- The ***Billing*** component is responsible for handling user charges, related activities and information. It consists of the following sub-components:
    - ***Charging***. The sub-component is responsible for performing usage measurements and user charging. It consists of two sub-components:
        - ***Usage Measurement*** that will monitor and measure service usage.
        - ***Billing Statements Creation*** that will handle user invoicing.
    - ***Reporting***. The subcomponent will deliver functionality to provide a user with usage reports. The details will give a transparency as for the resources consumed and, thus, money spent.

  - ***Usage Data.*** The sub-component data is generated by the Billing Statement Creation component and is required for user charging and reporting performed within Reporting component.
  - ***Service and Price data.*** The subcomponent data is generated by the Billing Statement Creation component as well as "Contracting" and "Data accessor" components, and is required for provisioning of the service and prices-related data.
- The ***Contracting*** component is responsible for contracting services with ACSmI and directly with CSP. It consists of the following sub-components:
  - ***Service Contract Registry.***
  - ***Contract Management.***
- The component ***Data Accessor*** is responsible for obtaining the required information/data from one CSP/service to be able to monitor it and to inform ADAPT with all the information that could require to (re)deploy the multi-cloud application through a connector manager. It has two related sub-components:
  - ***Accessor***, responsible for accessing data.
  - ***Migrator***, responsible for data migration.

Please see the detailed diagram below.

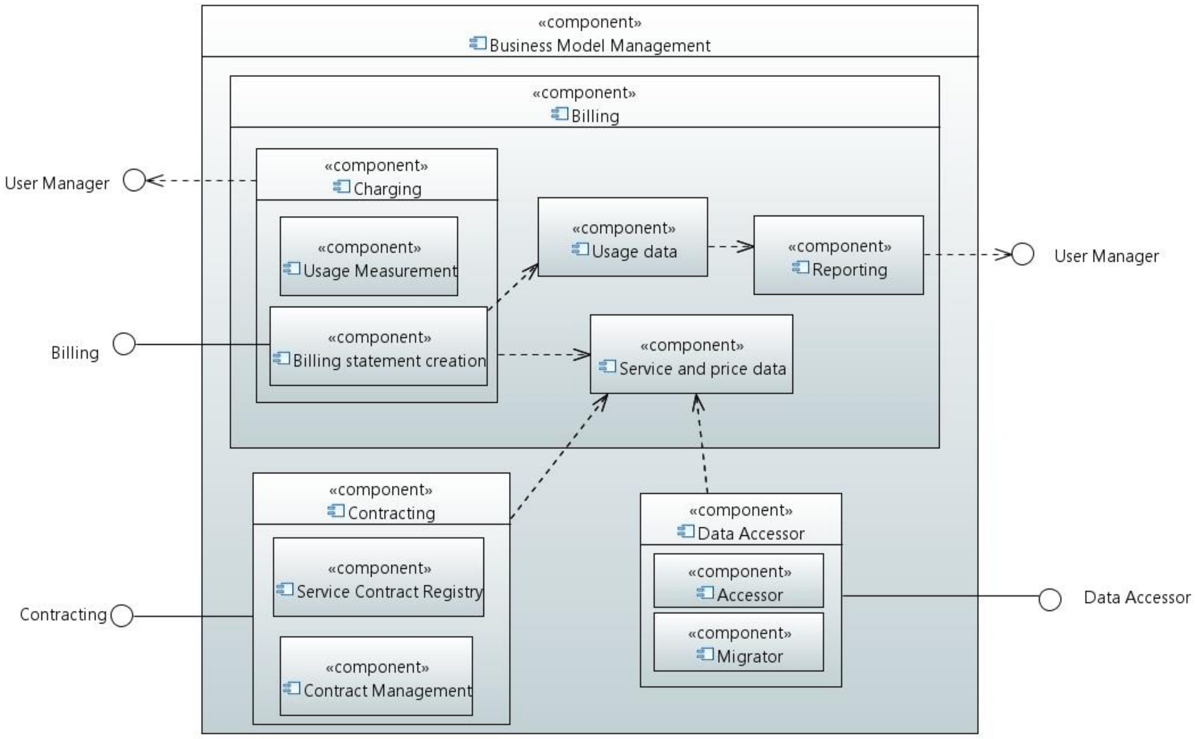
«component» Business Model Management
«component» Billing
«component» Charging
«component» Usage Measurement
«component» Billing statement creation
«component» Usage data
«component» Reporting
«component» Service and price data
«component» Contracting
«component» Service Contract Registry
«component» Contract Management
«component» Data Accessor
«component» Accessor
«component» Migrator
User Manager
Billing
Contracting
User Manager
Data Accessor

Figure 12: Business Model Management internal component diagram

7 Technologies to be used and deployment options

The deployment options for the services are based upon the availability of one or more platforms to deploy the individual components into, be this disperse cloud providers or different cloud platforms (regardless of vendor).

The deployment scenarios referenced give us a number of possibilities to test the DECDIDE toolset. These include but are not limited to:

- Deployment of services across multiple geographically dispersed cloud service providers;
- Deployment of services across different cloud technologies within a single cloud service provider;
- Deployment of services within a single cloud service provider in one technology.

The underlying technologies which support these uses case services are largely irrelevant, however the technologies are important in particularly to the ACSml and what virtualization technologies are supported (or proprietary software) to allow for a level of automation or orchestration.

At the time of writing, the ACSmI currently integrates with CSPs rather than technologies 'per se'. More concretely, these include:

- CloudSigma
- Amazon EC2

There are two approaches which can be taken to increase the adoption of the ACSml: 1) a technology based approach or 2) a CSP based approach. Ultimately particularly with the smaller CSPs the common used platform to facilitate IaaS service is VMWare. This is also true of businesses operating their own virtualization platforms.

The Figure below illustrates the domination of VM Ware across different business sizes as well as the adoption of variety of cloud technologies, not just one within a single business.

There is little data available around Cloud Vendor technology usage, particularly amongst the smaller players. There is less appetite or finances to invest on a grand scale into a new technology much in the same way that Microsoft, Google and Amazon have been able to do.

There have been small implementations of OpenStack by some Cloud Service Providers [41] and the Open Source nature of this means that a large number of existing tools within the DevOps paradigm are already compatible. The CSP market is dominated by the larger players as illustrated [42], so DECIDE needs to make pragmatic choices to ensure compatibility, and usage of their tools across a larger footprint.

The deployment options, which we referenced earlier, need to take into account the interoperability of the cloud environments and how they will be managed. This is a challenge that the ACSmI will need to address.

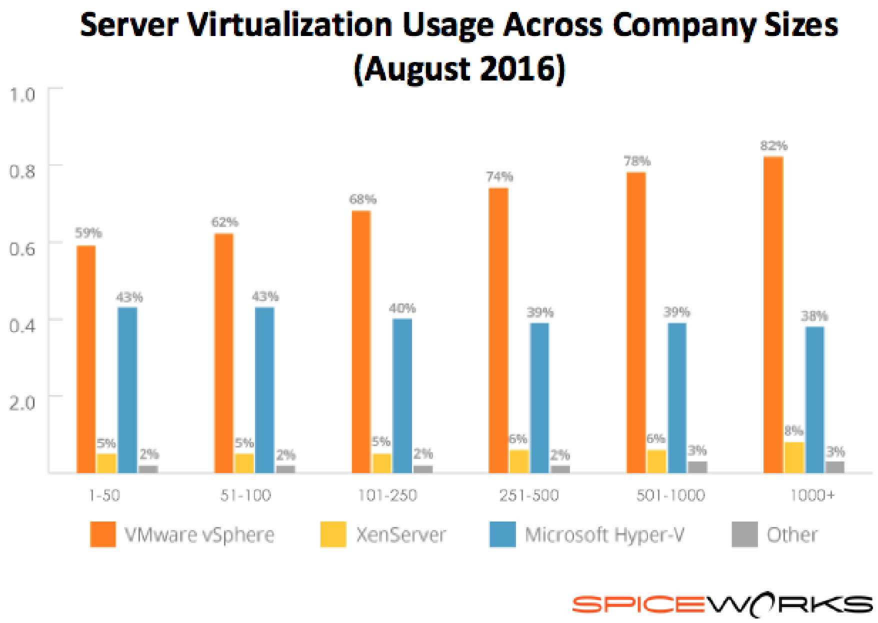

Figure 13: Server Virtualisation across company sizes [43]

8 Conclusions

This deliverable has collected the results obtained from the activities performed in the WP5 during the first 6 months of the DECIDE project.

This report has started with an analysis of the solutions existing today both in the market as well as in open source projects. This analysis also includes an extensive study on related standards as well as legislation initiatives on cloud SLAs and privacy As explained in section 2.1.1, there are some new features that need to be developed and other features that shall be extended.

The process to design the ACSmI is as follows: We have analysed the functional requirements based on the DoA approved by the European Commission. Then we continued with a high level design of the architecture and the main functionalities of the ACSmI as a whole. This can actually be found in section 3. Based on these main functionalities, we have derived the requirements for each main module and depicted the conceptual design of the ACSmI components. This design shows, on one hand the interfaces between the different components of the ACSmI and on the other, the external interfaces with other KRs of DECIDE like OPTIMUS and ADAPT.

Next steps for this workpackage are to select the technologies to develop the functionalities and to start with the development of the first prototype due month 12.

9 References

[1] DECIDE Consortium, "D2.1 Detailed requirements specification," 2017.

[2] Cloudmore, “Cloudmore CSB solution,” [Online]. Available: http://web.cloudmore.com/portal. [Accessed March 2017].

[3] Activeeon, “Automate, Accelerate & Scale: Workflows, Scheduling for IT and Scientists,” [Online]. Available: http://www.activeeon.com/. [Accessed May 2017].

[4] https://www.nimbix.net/, "Nimbix: High Performance Computing and Supercomputing Platform," [Online]. Available: https://www.nimbix.net/. [Accessed May 2017].

[5] Gompute, "Gompute: The HPC Cloud platform," [Online]. Available: https://www.gompute.com/. [Accessed May 2017].

[6] Cyclecomputing, "Cycle Computing Cloud Solutions: Better Answers. Faster," [Online]. Available: https://cyclecomputing.com/. [Accessed May 2017].

[7] NICE, "NICE: Usable Enterprise Grid & Cloud Solutions," 2017. [Online]. Available: https://www.nice-software.com/. [Accessed May 2017].

[8] UberCloud, "UberCloud: Cloud Simulation,CAE & HPC Services Platform," 2017. [Online]. Available: https://www.theubercloud.com/. [Accessed May 2017].

[9] Fortissimo, “Fortissimo project,” 2017. [Online]. Available: https://www.fortissimo-project.eu/. [Accessed March 2017].

[10] Bull atos Technologies, "Bull - extreme factory," [Online]. Available: https://bull.com/extreme-factory/. [Accessed May 2017].

[11] Atos Technologies, “Bull - bullx supercomputers,” [Online]. Available: https://bull.com/bullx-supercomputers/. [Accessed 5 2017].

[12] rescale, "Cloud HPC Simulation Platform," 2017. [Online]. [Accessed http://www.rescale.com/ May 2017].

[13] Cloudsigma, “CloudSigma Partners with CompatibleOne to Allow for a Unified View of Computing Environments Across Locations,” [Online]. Available: https://www.cloudsigma.com/cloudsigma-partners-with-compatibleone-to-allow-for-a-unified-view-of-computing-environments-across-locations/. [Accessed March 2017].

[14] Jamcracker, “Jamcracker Platform,” 2017. [Online]. Available: https://www.jamcracker.com/. [Accessed March 2017].

[15] ComputeNext, “ComputeNext: Cloud Brokerage And Marketplace Platform,” 2016. [Online]. Available: https://www.computenext.com/. [Accessed May 2017].

[16] Cloud28+ Hewlett Packard Enterprise, "Your Clouds of Clouds," 2017, [Online]. Available: https://cloud28plus.com/. [Accessed May 2017].

[17] Cloud Broker, "Cloud Broker," [Online]. Available: www.cloudbroker.com. [Accessed 05 April 2016].

[18] ETSI, "Cloud Standards Coordination," European Telecommunication Standardization Institute, 28 January 2016. [Online]. Available: http://csc.etsi.org/. [Accessed 10 March 2017].

[19] ETSI, "Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards," Europen Telecommunication Standardization Institute, Sophia Antipolis, France, 2016.

[20] "cloud-standards.org," 15 November 2015. [Online]. Available: http://cloud-standards.org/wiki/index.php?title=Main_Page. [Accessed 10 March 2017].

[21] CloudWatch II project, "http://www.cloudwatchhub.eu," 2017. [Online]. Available: http://www.cloudwatchhub.eu. [Accessed 10 March 2017].

[22] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 17788:2014: Information technology -- Cloud computing -- Overview and vocabulary,* Geneva, Swizerland, 2014.

[23] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 17789:2014: Information technology -- Cloud computing -- Reference architecture,* Geneva, Swizerland, 2014.

[24] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 19086-1:2016: Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts,* Geneva, Switzerland, 2016.

[25] International Organisation for Standardization/International Electrotechnical Commission, *ISO/CD 19086-2: Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model,* 2016.

[26] Open Grid Forum, *GFD-R.192: Web Services Agreement Specification (WS-Agreement),* 2011.

[27] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (2nd edition),* Geneva, Swizerland, 2013.

[28] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services,* Geneva/Switzerland, 2015.

[29] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors,* Geneva/Swizerland, 2014.

[30] International Organisation for Standardization/International Electrotechnical Commission, *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (second edition),* Geneva, Switzerland, 2013.

[31] Cloud Security Alliance, *Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union,* 2013.

[32] Cloud Security Alliance, *Cloud Controls Matrix,* 2016.

[33] Cloud Security Alliance, *CTP Data Model and API, rev. 2.13,* 2015.

[34] "Open Cloud Computing Interface," Open Grid Forum, [Online]. Available: http://occi-wg.org/about/specification/. [Accessed 02 05 2017].

[35] Organization for the Advancement of Structured Information Standards, *Cloud Application Management for Platforms (CAMP) Test Assertions Version 1.1,* Jacques Durand, Gilbert Pilz, Adrian Otto, Tom Rutt ed., 2014.

[36] Distributed Management Task Force, *Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol,* 2012.

[37] Organization for the Advancement of Structured Information Standards, *Topology and Orchestration Specification for Cloud Applications Version 1.0. 25,* Derek Palma, Matt Rutkowski, Thomas Spatzier ed., 2016.

[38] The Storage Networking Industry Association, *Cloud Data Management Interface (CDMI),* 2015.

[39] University of Stuttgart, "HLRS High Performance Computing Center Stuttgart," 2016, [Online]. Available: https://www.hlrs.de/home/. [Accessed May 2017].

[40] DECIDE Consortium, «D6.1 Initial Use Case Requirements Capture,» 2017.

[41] OpenStack, "Public Clouds," OpenStack, [Online]. Available: https://www.openstack.org/marketplace/public-clouds/.

[42] Channele2e, "Cloud Market Share 2017," [Online]. Available: https://www.channele2e.com/2017/02/09/cloud-market-share-2017-amazon-microsoft-ibm-google/.

[43] P. Tsai, "Server Virtualization and OS Trends," Spice Works, August 2016. [Online]. Available: https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends. [Accessed April 2017].