Federated Cloud Service Broker (FCSB): An Advanced Cloud Service Intermediator for Public Administrations

Juncal Alonso Ibarra, Leire Orue-Echevarria, Marisa Escalante, Gorka Benguria
and Gorka Echevarria
Tecnalia Research and Innovation, Parque Científico y Tecnológico de Bizkaia, Edificio 700, 48160 Derio, Bizkaia, Spain

Keywords: SLA, QoS, Cloud Services, Cloud Service Broker, Services Aggregation, Cloud Service Intermediator, Technical Design.

Abstract: A cloud services brokerage is third-party software that adds value to cloud services on behalf of cloud service consumers. Their goal is to make the services more specific to a company, or to integrate or aggregate services, to enhance their security, or to do anything which adds a significant layer of value (i.e. capabilities) to the original cloud services being offered (Plummer, 2012). There exist several solutions focused on providing service brokerage of Cloud Service Providers (CSP), mainly VM's and virtualized resources, but not of other services offered (e.g. Data Processing as a Service) or SaaS applications which are certified and legally compliant. This paper proposes a solution for a Federated Cloud Service Broker (FCSB) overcoming existing challenges in the public sector such as Governance, Interoperability and portability, SLAs compliance and assessment, Intelligent discovery of cloud services, cross border interoperability and legislation awareness . The analysis of the existing solutions, and the presentation of the approach made in (Alonso, et al., 2016) is complemented with a technical design including the main functionalities and the modules that will implement them.

1 INTRODUCTION

The digital transformation from product to service economy means changes in the companies' operating environment: they need to transform into service providers from product providers and be able to flexibly change their role in the value chain and markets. In order to be able to foster the change, the companies IT infrastructure needs to be more flexible. Cloud services enable this to some degree, but as such create dependency to external partners for a company. In a world where new players come, others disappear, and conditions are continuously changing, how can the companies be sure that the architectural decisions that were taken in the past continue to be the best one? The decision on using one, another, or several approaches simultaneously is driven by certain evaluation criteria (e.g. profitability, reliability, performance, security, legal or even ecological aspects). There are several multi-cloud solutions available for solving specific problems, but to date, little attention has been paid to distributing the cloud risk, and managing multiple clouds from a single technology platform. Working with many CSPs means managing multiple relationships (Alonso, et al., 2016). Most enterprises are already negotiating multiple contracts with multiple CSPs and multiple contracts mean multiple service level agreements, multiple payments, multiple passwords, multiple data streams, and multiple providers to check up on. That leads to questions about how to make those services work together, or how to unify all the efforts so maximum effectiveness and efficiency can be obtained. This is when a Cloud Service Broker (CSB) comes into play. Gartner defines a cloud services brokerage as a third-party software that adds value to cloud services on behalf of cloud service consumers (Gartner, 2016). Their goal is to make the service more specific to a company, or to integrate or aggregate services, to enhance their security, or to do anything which adds a significant layer of value (i.e. capabilities) to the original cloud services being offered. Consumers can leverage solutions offered by CSBs that allow organizations to focus on other pressing business needs instead (Gartner, 2012).

Ibarra, J., Orue-Echevarria, L., Escalante, M., Benguria, G. and Echevarria, G.
Federated Cloud Service Broker (FCSB): An Advanced Cloud Service Intermediator for Public Administrations.
DOI: 10.5220/0006285003840391
In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 356-363
ISBN: 978-989-758-243-1

Existing cloud services shall be made available dynamically, broadly and cross border, so that software providers can re-use and combine cloud services, assembling a dynamic and re-configurable network of interoperable, legal compliant, quality assessed (against SLAs) single and composite cloud services.

1.1 Main Challenges to Be Solved

With so much activity implementing front-end and back-end applications in public, private and hybrid clouds, complexity has grown at every level (business, application, transaction and regulatory) (Fisher, 2014). To generate meaningful results, it is envisioned that public administrations (PAs) need to address key challenges in the next years (Fisher, 2014) (AGID, 2015):

1. Governance: Ensuring that services deployed in the cloud are protected is critical. Fostering strong governance programs in place will protect enterprises and their data.
2. Risk tolerance. Every enterprise should assess their tolerance for pitfalls such as lost data and application outages.
3. Regulations. Lobbying for regulations and standards are predicted to be a key step to ensure cloud integration.
4. Cross border interoperability. Context-aware service management and fluid service integration, assuring data portability, while guaranteeing proper identity propagation with service-specific granularity level of information.
5. Matching customer requirements with cloud service specifications. This implies that the selected service offerings must match with all functional and non-functional requirements (NFR) coming from the customers.
6. Legislation compliance. A big challenge in this concern is to develop the methods and interfaces for securing legislation compliance and easy legislation change propagation in a legislation heterogeneous environment.
7. Cloud service SLA assessment and monitoring. Monitor and control the diverse properties of utilized services, composite or stand-alone, at real-time, especially when SLA conditions are not fulfilled (e.g. elasticity, data localisation).
8. Seamless change of provider. Enable to seamlessly change the service provider including all services, dependencies and associated data to avoid vendor lock-in and to be able to quickly react in situations like bankruptcy of the cloud provider or any other cases which causes outage of the service.

This paper proposes a solution for a FCSB overcoming these challenges. The paper is organized as follows. First, an analysis of the state of the art is presented, and then it proceeds with the description of the high level architecture of the solution and the functionalities to be covered. It also presents the different deployment options and technologies to be used, as well other relevant aspects considered (portability, standards, resilience and performance).

The paper finishes with a set of conclusions and next steps to follow.

2 STATE OF THE ART AND TECHNOLOGY: SOLUTIONS FOR CLOUD SERVICES BROKERS

A cloud service broker has several main goals:

- To hide the heterogeneity of cloud APIs.
- To add improved functionality that helps to get a unified view of all the clouds used and all the resources in them.
- To offer a repository of cloud services or cloud marketplaces

In the following section, the current solutions to cover these main goals are presented. The solutions presented can be classified as commercial cloud services market place, Open Source services market place and Government cloud marketplaces. Moreover, some solutions developed in different research projects are presented.

2.1 Analysis of Current Solutions

Among the commercial and open source cloud services market place the following solutions are found:

- AWS (Amazon, 2015) Marketplace includes developer tools, software infrastructure, business software, and Desktop applications.
- HPE Helion (HP, 2015) provides functionalities for IT spending related to the contracted cloud services, service performance, operational configurations and security features.
- IBM (IBM, 2015) marketplace offers services classified in four different types: Application, Business Process, Infrastructure and Platform.

- Appcara AppStack (Appcara, 2015) allows users to easily deploy and manage new multi-tiered applications or migrate existing applications running on physical or virtual servers, into a choice of cloud targets.
- Jamcracker Service Delivery Network (Jamcracker, 2016) enables organizations to create, deliver, and manage multi-cloud services and implement a cloud-enabled business model for offering, delivering, supporting and billing for cloud services.
- Cloud broker (Cloud Broker, 2016) platform is a middleware and application store for compute intensive applications in the cloud.
- Juju (Ubuntu, 2015) allows software to be deployed, integrated and scaled on a wide choice of cloud services or servers.

At the same time, Government cloud marketplaces continue to growth in number and influence. For example, Gov.apps (US Government, 2015) and UK Digital Marketplace (UK Government, 2016) act as cloud services catalogue.

Also EU funded projects have been working in this direction:

- ARTIST (ARTIST Consortium, 2016) has developed a benchmarking tool to select the most suitable cloud provider as part of its migration tool-suite.
- CELAR (European Comision, 2016) provides automatic, multi-grained resource allocation for cloud applications.
- Mosaic (mOSAIC Consortium, 2016) offers cloud developers, maintainers and users to specify the service requirements in terms of a cloud ontology and communicate them to the platform via the provided API.
- Strategic (Strategic Consortium, 2016) Service Store acts as a marketplace for developers that want to publish their applications for eGovernment.
- BEACON (Beacon Consortium, 2016) defines and implements a federated cloud network framework that enables the provision of federated cloud infrastructures, with special emphasis on intercloud networking and security issues.
- Cloud28+ (Cloud28, 2016) offers a catalogue of trusted, business cloud services that matches in-country or cross-border buyer and regulatory workload requirements.

2.2 Key Functionalities Covered by the Existing Solutions

Most of presented solution are mostly focused on providing service brokerage of cloud service providers, mainly VM's and virtualized resources, but not of other services offered (e.g. Data Processing as a Service) or SaaS applications which are certified and legally compliant.

The Table 1, below, presents how the key functionalities are covered (F: fully; P: Partially; N: Not covered).

Table 1: Matrix of the analysed solutions vs. main requirements.

Solution name	**Interoperability**	**Customer requirements**	**Change of service providers**	**SLA assessment and monitoring**	**Legislation of EU countries**	**Portability**	**Standards**	**Interoperable Authentication**
Amazon WS	P	P	N	P	N	P	P	P
HP	N	F	P	P	N	P	P	P
IBM	P	P	N	F	N	P	F	p
AppStack	P	F	P	P	N	F	F	P
Jamcracker	P	F	P	F	N	P	P	F
Juju	N	P	P	F	N	F	P	P
Helix Nebula	P	P	P	N	N	P	P	P
Cloud Broker		P	P	P	N	P	P	F
Gov.apps	P	P	N	N	N		P	N
UK Digital Marketplace	N	F	P	N	N	P	P	F
ARTIST	N	F	N	F	N		P	N
CELAR	P	P	P	P	N	P	P	P
Mosaic	P	P	F	N	N	F	N	P
Strategic	P	P	P	F	N	P	P	P
BEACON	P	P	P	P	N	F	F	F
Cloud28+	F	P	P	F	P	P	P	N

Most of the offering is not targeting the public sector, where specific challenges may arise (Alonso, et al., 2016). There does not exist a unified framework, with a reference architecture covering specific challenges faced by the PAs such as the compliance with regulatory aspects, the assessment of NFP of the cloud services, or the seamless and secure change of CSP (including cross-border interoperability).

3 FEDERATED CERTIFIED SERVICE BROKERAGE (FCSB) FOR PUBLIC ADMINISTRATIONS: A PROPOSED SOLUTION

3.1 High Level Architecture

Before the high level architecture is described, it is needed to detail certain assumptions that were made during the definition of the technical design. These are important as some requirements were not explicitly stated. These assumptions are stated next:

- External FSCB with which the proposed FSCB will interact, are designed following the same proposed architecture.
- When describing federated processes/components, we have assumed that external FCSBs are considered as a CSP.
- The services to be offered by the FCSB to the PAs, are discovered from the ones already endorsed in its own service registry or in the service registry of external FCSBs.
- The discovery of cloud services from external FCSBs will be launched by the PAs.
- Cloud services from external FCSBs will be only be discovered in the FCSBs registered as users in the user registry.
- Changes in the legislation will be monitored outside the FCSB by legal experts. The changes and updates will be introduced into the corresponding registry by those experts.
- The user interface (Dashboard) will be automatically customized for the different users based on their assigned roles, accessing only to the allowed actions.

There are seven main components in charge of implementing the core functions of the FCSB. A high level description of these components and their sub-components is presented next (see Figure 1.):

1. Service Management: This core component is in charge of executing and manag all the operations related to the services offered by the FCSB. 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:

1.a. Service Registry is in charge of registering all the information related to the services offered by the FCSB. Information such as: service id, related provider, legislation covered, SLAs, CSP id, etc. is stored and updated in the Service Registry.

1.b. Service Registry Governance is responsible for managing the access and update to the service registry.

1.c. User Service Requests is in charge of managing the requests from the users when discovering the services. It gathers and processes the requirements from the users when discovering services in the FCSB.

1.d. Service Composition manages the composition of different services from different/or the same CSPs, managing the composed CSLA and other aspects related to the composition.

1.e. Service Operation Management is in charge of the management of the operation itself, the CSLA creation monitoring and assessment and the metering

1.f. Intelligent Service Discovery is the one in charge of managing the Intelligent Service Discovery of services in the FCSB as well as the service benchmarking, that is, the classification of the services according to the requirements demanded by the end-user.

2. User Management controls all the activities related to the different users of the FCSB. The sub-modules included in the User Management are:

2.a. Roles Manager manages the activities related to the roles in the FCSB (creation, modification, assignment, deletion).

2.b. Policy Manager manages the activities related to the policies in the FCSB (creation, modification, assignment, deletion).

2.c. User Manager manages the activities related to the users in the FCSB (creation, modification, roles assignment, deletion).

2.d. User Registry stores all the information associated to the users of the FCSB.

2.e. Authentication Manager performs the authentication of the users and manages the access to the different actions/functions of the FCSB for each user.

3. Service Contract Management is in charge of executing and manages all the operations related to Service Contracts in the FCSB. The sub-modules included in the Service Management are:

3.a. Contract Manager manages mainly two different types of contracts: The contracts between the PAs (service consumers) and the FCSB and the

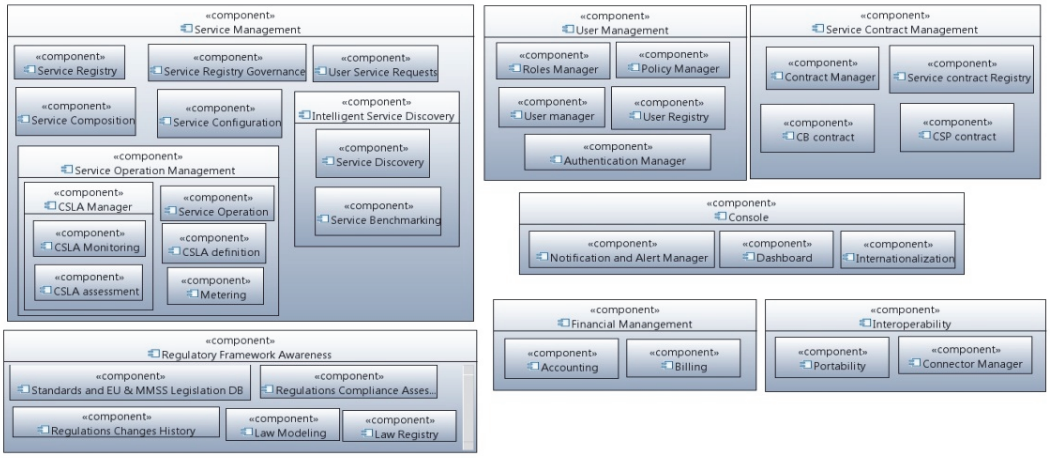
«component» Service Management
«component» Service Registry
«component» Service Registry Governance
«component» User Service Requests
«component» Service Composition
«component» Service Configuration
«component» Intelligent Service Discovery
«component» Service Discovery
«component» Service Benchmarking
«component» Service Operation Management
«component» CSLA Manager
«component» CSLA Monitoring
«component» CSLA assessment
«component» Service Operation
«component» CSLA definition
«component» Metering
«component» Regulatory Framework Awareness
«component» Standards and EU & MMSS Legislation DB
«component» Regulations Compliance Asses...
«component» Regulations Changes History
«component» Law Modeling
«component» Law Registry
«component» User Management
«component» Roles Manager
«component» Policy Manager
«component» User manager
«component» User Registry
«component» Authentication Manager
«component» Service Contract Management
«component» Contract Manager
«component» Service contract Registry
«component» CB contract
«component» CSP contract
«component» Console
«component» Notification and Alert Manager
«component» Dashboard
«component» Internationalization
«component» Financial Manangement
«component» Accounting
«component» Billing
«component» Interoperability
«component» Portability
«component» Connector Manager

Figure 1: FCSB high level architecture.

contracts between the CSPs (service providers) and the FCSB.

3.b. Service Contract Registry stores the different contracts existing in the FCSB.

3.c. *CloudBroker Contract* manages the contracts with the PAs and the related actions.

3.d. CSP Contract manages the contracts with the CSPs.

4. Console is the module in charge of implementing the interface with the different users in the FCSB. The sub-modules included in the Console are:

4.a. Notification and Alert Manager manages the different alerts and notification shown to the user.

4.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.

4.c. Internationalization allows the internationalization of the GUI so that the FCSB can be used in different languages.

5. Interoperability is in charge of performing the portability between different services of different or the same CSP and the communication with the CSPs and with other FCSBs. The sub-modules included are:

5.a. Portability is responsible for the coordination and execution of the data portability between two services.

5.b. Connector Management manages the different connectors of the different services form diverse CSPs. This sub-module also manages the communication with other external FCSBs.

6. Financial Management is in charge of performing the activities related to the financial operations with the different users of the FCSB. It manages the payments to the CSPs and the receipts to the PAs. The sub-modules included in the Financial Management module are:

6.a. Accounting is responsible for calculating the total values for billing PAs for the services users and paying the CSPs for the services used.

6.b. Billing generates the bills for the users.

7. Regulatory Framework Assessment is in charge of assessing the compliance of the services with the different legislations. The sub-modules included are:

7.a. Regulations Compliance Assessment 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 FCSB.

7.b. Law Registry stores the information of the different legislations to be considered in the FCSB.

7.c. Regulations Change History stores the changes suffered by the different legislations (i.e. updates, new versions, etc.)

7.d. Law Modelling allows the legal experts to model the different legislations so that the legislations assessment can be done in the FCSB.

3.2 Main Functionalities

In this section we present the different processes that will take place in the FCSB. We have classified them following the cloud service process lifecycle. Different approaches have been used to define the lifecycle of a cloud Service. (SLA Ready Consortium, 2015) (BMC Software, 2010).

In the FCSB, the service will pass through the following phases and processes:

- Service initialization, including cloud service endorsement into the broker, (Federated) intelligent discovery of services, (Federated) service contracting, CSLA provision, users management, security management and creation of the aggregated services in the FCSB.

- Service operation, including CB CSLA monitoring, legislation compliance due to changes in the legislation, data migration/portability, service metering, billing to the user, and CP costs estimation.
- Service termination: including service withdrawal and service contract termination

3.3 Deployment Options and Technologies to Be Used

There are different elements to consider when deciding the deployment of the presented solution, and the technologies to be used:

- Resources
- The application architecture and stage (monolithic, modular, service oriented, layered)
- The forecasted demand and its possible evolution
- Additional NFRs, such as profitability, high-availability, scaling, etc.

Taking all the above into account, it is important to focus the application architecture and development towards the most flexible result. We need an application that is capable to be deployed anyway, anywhere and supported by anyone. And an application that is prepared to scale and provide additional NFRs.

To achieve that purpose we envision to:

- Implement a micro-cloud approach: split the application in components and place each component in a container. This will allow in the future scaling independently each component.
- Package the code in installable binaries *.deb, *.rpm, etc.
- Use popular technologies: Those with a significant user base.
- Avoid vendor locking: Avoid proprietary solutions with vendor locking effects. And in case, there is no alternative, wrap the vendor locking technology or XaaS.
- Split since the beginning those components that are subject to XaaS, i.e. databases, notification, storage, etc.
- Focus on technologies that can be used by many instances of the same component: databases, memcached, object storage, block storage servers.
- Decouple as much as possible also in data: avoid big databases; differentiate between static, dynamic and temporal information; do not share databases among components; minimize information writing and centralize that writing in one component.

Besides, during the development we propose to use a DevOps approach to streamline the development and systematize the operation and maintenance activities.

Summarizing the list of technologies proposed to the implementation of the design contained are:

- Mature and highly used programming languages: Java, Javascript, Python, PHP.
- Dependency management technologies such as maven for java, or distutils and set up tools for python.
- Repository (Git or svn) for application code, configuration, installation binaries or infrastructure specification.
- Package management systems such as apt-get or yum
- Container technologies such as docker, openshift, cloudfoundry, …
- Database for information storage relational or non-relational
- Cache technologies, such as memcached or redis, technologies when possible

3.4 Other Aspects of the FCSB Solution

PAs need to be enabled to seamlessly change the service provider including all services, dependencies and associated data to avoid vendor lock-in and to be able to quickly react in situations like bankruptcy of the cloud provider or any other cases which causes outage of the service. This imposes to adhere to existing and established standards, standard interfaces, paradigms and certifications.

In the proposed technical design the seamless change of cloud provider, that is, the portability between two different providers will be supported by the Intelligent Service Discovery module and the Interoperability module. These modules, and therefore, the FCSB will support the following standards: CDMI (SNIA, 2016) , OCCI (OCCI Working Group, 2011), TOSCA (OASIS, 2015), IEEE P2301: P2302 (IEEE, 2016).

For the FCSB to be adopted by European Public Administrations, the FCSB must be aligned and comply with EU standards and existing legislation.

Regarding the compliance with the existing legislation at this first stage the main focus has been to model and accomplish as much as possible the following legislation: General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 (European Comision, 2016)), and the ePrivacy directive (Directive on Privacy and Electronic Communication (EUR LEX, 2002)).

Resilient computing is a form of failover that distributes redundant implementations of IT resources across physical locations. IT resources can be pre-configured so that if one becomes deficient, processing is automatically handed over to another redundant implementation. Within cloud computing, the characteristic of resiliency can refer to redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds. Cloud consumers can increase both the reliability and availability of their applications by leveraging the resiliency of cloud-based IT resources

Given the criticality both in terms of availability and performance, it has been opted for a deployment architecture in which the FCSB will be replicated in at least two cloud providers. This will permit to ensure both the availability and the compliance of the service with the established SLAs all time. In order to ensure the compliance of FCSB with all NFRs, there will be used tools that will be continuously monitoring specific metrics related to these requirements, so that when the value of some of them increases or decreases depending on the agreed criteria, the needed actions to ensure the quality of service will be taken.

Another critical aspect for FCSB to be taken up, the user experience is of great importance. Under this respect, the following practices have been considered as critical in the case of FCSB:

- Client-Aware Cloud Computing: One way to ensure that end users have the best possible experience is to provide cloud applications that are able to run partially on the client device itself.
- Application Performance Management: The only real way to monitor the performance of your cloud-based applications is through the real experience of end users. Having full and real-time visibility of the end user experience and application performance is essential to preventing a cloud nightmare.
- Plan B – Cloud Backup and Alternate Servers: Another aspect to optimize as much as possible the execution of applications, will be the provision of contingency measures in case of system failure. There are mechanisms that redirect the processing to other computing and storage nodes so that the end user does not perceive these problems in case they occur.

4 CONCLUSIONS

This paper presents how the authors envision the design, implementation, functionalities, and features of the FCSB. The technical design of the FCSB, presented in this paper, tries to overcome the specific challenges to be faced by the PAs, such as governance, risk tolerance, legislation compliance, regulations, cross border interoperability, management of the citizens' requirements, SLAs assessment, and seamless change of provider.

The next activities include the actual implementation of the pilot of the technical design presented. For that, the authors will follow an iterative and incremental approach based on SCRUM and in alignment with a DevOps philosophy. The prioritisation of the functionalities will come from the priority analysis of functional requirements. A continuous integration environment accompanied by a source code management will be set up to ensure the quality of the produced code. Integration, Quality and Deployment will be performed continuously following the DevOps approach, commonly used in the context of cloud-based applications

ACKNOWLEDGEMENTS

The projects leading to this paper (Cloud For Europe) has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration and from European Union's Horizon 2020 research and innovation programme under grant agreement No 731533.

REFERENCES

AGID, 2015. *AGID GOV.* [Online] Available at: http://www.agid.gov.it/sites/default/files/documentazione/annex_iv_a_-_challenges_and_general_requirements_v103_publish_0_0.pdf[Accessed 2016].

Alonso, J., Orue-Echevarria, L. & Escalante, M., 2016. *Transformational Cloud Government (TCG):*

Transforming Public Administrations with a Cloud of Public Services. Madrid, Elsevier.

Alonso, J., Orue-Echevarria, L., Escalante, M. & Benguria, G., 2016. *Empowering Services Based Software in the Digital Single Market to Foster an Ecosystem of Trusted, Interoperable and Legally Compliant Cloud-services.* Rome, SCITEPRESS.

Amazon, 2015. *AWS Marketplace.* [Online] Available at: https://aws.amazon.com/marketplace [Accessed 21 05 2015].

Anon., s.f. s.l., s.n.

Appcara, 2015. *AppStack Company.* [Online] Available at: http://www.appcara.com/products/appstack/ [Accessed 21 05 2015].

ARTIST Consortium, 2016. *ARTIST Project.* [Online] Available at: http://www.artist-project.eu/[Accessed 30 09 2016].

Beacon Consortium, 2016. *BEACON Project.* [Online] Available at: http://www.beacon-project.eu/[Accessed 30 09 2016].

BMC Software, 2010. *Cloud Lifecycle Management,* s.l.: s.n.

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

Cloud28, 2016. *Europe´s Cloud of Clouds.* [Online] Available at: http://www.cloud28plus.eu/[Accessed Septembre 2016].

EUR LEX, 2002. *EUR LEX.* [Online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML[Accessed 18 11 2016].

European Comision, 2016. *CORDIS.* [Online] Available at: http://cordis.europa.eu/project/rcn/105163_es.html [Accessed 30 09 2016].

European Comision, 2016. *European Comision Justice.* [Online] Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf[Accessed 18 11 2016].

Fisher, D., 2014. *Oracle.* [Online] Available at: http://www.oracle.com/us/solutions/cloud/managed-cloud-services/makingwaves-final-2162934.pdf[Accessed 2016].

Gartner, 2012. *The Business Landscape of Cloud Computing.* [Online] Available at: https://www.cloudeassurance.com/white-papers/Gartner_Daryl_Plummer_and_Financial_Times_e-Book_The_Business_Landscape_of_Cloud_Computing.pdf[Accessed 17 November 2016].

Gartner, 2016. *Cloud Services Brokerage.* [Online] Available at: http://www.gartner.com/it-glossary/cloud-services-brokerage-csb/ [Accessed 17 November 2016].

HP, 2015. *HP Helion.* [Online] Available at: https://marketplace.hpcloud.com/[Accessed 21 May 2015].

IBM, 2015. *IBM Cloud.* [Online] Available at: http://www.ibm.com/cloud-computing/us/en/marketplace.html[Accessed 21 May 2015].

IEEE, 2016. *IEEE Standards Association.* [Online] Available at: Available: https://standards.ieee.org/develop/project/2302.html[Accessed 27 09 2016].

Jamcracker, 2016. *Jamcracker Services Delivery Network.* [Online] Available at: http://www.jamcracker.com/jamcracker-services-delivery-network-jsdn[Accessed March 2016].

mOSAIC Consortium, 2016. [Online] Available at: http://www.mosaic-cloud.eu/[Accessed 30 09 2016].

OASIS, 2015. *TOSCA.* [Online] Available at: https://www.oasis-open.org/committees/tosca [Accessed 25 05 2015].

OCCI Working Group, 2011. *Open Cloud Computing Interface - Core,* s.l.: OCCI.

Plummer, D., 2012. *Forbes.* [En línea] Available at: http://www.forbes.com/sites/gartnergroup/2012/03/22/cloud-services-brokerage-a-must-have-for-most-organizations/#3138aa2a52aa[Último acceso: 20 11 2016].

SLA Ready Consortium, 2015. *SLA Ready.* [Online] Available at: http://www.sla-ready.eu/cloud-sla-lifecycle[Accessed 27 09 2016].

SNIA, 2016. *Cloud Data Management Interface (CDMI).* [Online] Available at: http://www.snia.org/cdmi [Accessed 27 09 2016].

Strategic Consortium, 2016. *Strategic Consortium.* [Online] Available at: http://strategic-project.eu/ [Accessed 30 09 2016].

Ubuntu, 2015. *Ubuntu Juju,.* [Online] Available at: http://community.ubuntu.com/[Accessed 21 05 2015].

UK Government, 2016. *UK Digital Marketplace.* [Online] Available at: https://www.digitalmarketplace.service.gov.uk/[Accessed 30 09 2016].

US Government, 2015. *Gov.apps.* [Online] Available at: www.apps.gov[Accessed 21 05 2015].