Requirements and Architecture of a Cloud Broker

Activity 6: Integration and Experimentation
WP 6.4: Cloud Brokerage

<table>
<thead>
<tr>
<th>Due Date:</th>
<th>M12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submission Date:</td>
<td>31/05/2011</td>
</tr>
<tr>
<td>Start Date of Project:</td>
<td>01/06/2010</td>
</tr>
<tr>
<td>Duration of Project:</td>
<td>36 months</td>
</tr>
<tr>
<td>Organisation Responsible for the Deliverable:</td>
<td>BT</td>
</tr>
<tr>
<td>Version:</td>
<td>1.0</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Author(s):</td>
<td></td>
</tr>
<tr>
<td>Srijith K. Nair</td>
<td>BT</td>
</tr>
<tr>
<td>Pramod Pawar</td>
<td>City University</td>
</tr>
<tr>
<td>Ali Sajjad</td>
<td>City University</td>
</tr>
<tr>
<td>Mariam Kiran</td>
<td>University of Leeds</td>
</tr>
<tr>
<td>Ming Jiang</td>
<td>University of Leeds</td>
</tr>
<tr>
<td>Reviewer(s):</td>
<td></td>
</tr>
<tr>
<td>Ana Juan</td>
<td>ATOS</td>
</tr>
<tr>
<td>Johan Tordsson</td>
<td>Umeå</td>
</tr>
</tbody>
</table>
## Project co-funded by the European Commission within the Seventh Framework Programme

### Dissemination Level

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>Public</td>
</tr>
<tr>
<td>PP</td>
<td>Restricted to other programme participants (including the Commission)</td>
</tr>
<tr>
<td>RE</td>
<td>Restricted to a group specified by the consortium (including the Commission)</td>
</tr>
<tr>
<td>CO</td>
<td>Confidential, only for members of the consortium (including the Commission)</td>
</tr>
</tbody>
</table>

© OPTIMIS Consortium
This is a public deliverable that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons http://www.creativecommons.org

Full licensing information is contained in Annex A.
Table of Contents

1 EXECUTIVE SUMMARY .............................................................................................................. 1

2 INTRODUCTION ...................................................................................................................... 2

2.1 PURPOSE .............................................................................................................................. 2

2.2 GLOSSARY OF ACRONYMS ............................................................................................ 2

3 USE CASE SCENARIO ............................................................................................................. 3

3.1 STORYBOARD ...................................................................................................................... 3

3.2 ACTORS INVOLVED IN THE USE CASE ............................................................................ 5

4 BUSINESS CASE .................................................................................................................... 6

4.1 ANALYSIS OF THE MARKET ............................................................................................. 6

4.2 EXPECTED MARKET GROWTH ......................................................................................... 6

4.3 EXPLOITATION PLAN .......................................................................................................... 7

5 STATE OF THE ART ................................................................................................................ 9

6 EXPECTED INNOVATION ......................................................................................................... 11

7 REQUIREMENTS ANALYSIS .................................................................................................. 12

7.1 IDENTIFIED FUNCTIONAL REQUIREMENTS .................................................................... 12

7.1.1 SP using Multi-cloud services .................................................................................... 12

7.1.2 SP using Broker .......................................................................................................... 13

7.2 GAP ANALYSIS .................................................................................................................. 15

8 HIGH-LEVEL DESIGN .......................................................................................................... 16

9 CONCLUSION .......................................................................................................................... 20

10 REFERENCES ......................................................................................................................... 21

ANNEX A. LICENSE CONDITIONS .......................................................................................... 22

ANNEX B. RISK ASSESSMENT ANALYSIS ............................................................................ 24
Index of Figures

Figure 1: Cloud Broker ecosystem showing the players involved ........................................... 3
Figure 2: Diagrammatic representation of the Cloud Aggregation Ecosystem ...................... 5
Figure 3: Functional components of a cloud service broker providing brokerage services between multiple cloud providers. ........................................................................................................ 17
Figure 4: Component Interaction for risk assessment in private cloud .................................. 24
Figure 5: Component Interaction for risk assessment in cloud bursting ............................... 25
Figure 6: Component Interaction for risk assessment in federation of clouds ...................... 26
Figure 7: Component Interaction for risk assessment in multi-cloud .................................... 26

Index of Tables

Table 1: Comparison of Broker components and OPTIMIS Toolkit components ................. 19
1 Executive Summary

This deliverable presents a report on the work performed on the WP6.4 for the definition and analysis of the Cloud Broker Use Case. This work has been focused in three aspects: the description and refinement of the use case definition, the analysis of the business aspects related to the use case and finally, the analysis of the technical aspects of the use case, including the proposal of a high-level design.

In the first part, we describe the use case in detail, providing details on how the cloud broker works and what the key issues we will be considering in the activities associated with this work package. The second part tackles the business aspects related to the Cloud Broker use case. Cloud markets are expected to grow rapidly during next couple of years, presenting great business opportunities. According to Gartner and 451 GROUP, several cloud computing areas will see considerable growth, including the on-ramp markets which are closely related with our use case. Moreover, the use case is expected to show important innovations compared with the current practices and solutions in terms of providing requirements-functionality matching, choosing Infrastructure Provides based on parameters like trust, risk and eco-efficiency, in addition to cost.

Finally, the third part of the work analyzes the use case from a technical point of view. We explore the use case scenario for identification of additional requirements for the OPTIMIS toolkit to support the implementation of innovative value-added services presented in this document. Using these requirements and the description of the use case, we also propose a high-level design of the Cloud Broker.
2 Introduction

The D6.4.1 document provides an architectural design for brokerage based collaboration oriented multiple cloud provider use case scenario. The cloud broker is one of the core use cases that form part of the three Activity 6 use cases. A brief overview of the document follows.

The rest of this section defines the purpose of this document and provides a glossary of acronyms. Section 3 describes the use case scenario being considered in this work package while section 4 provides the business case in support of activities carried out in this work package including analysis of market and its growth potential. In section 5 we consider the state of the art in services that are similar to the one proposed in this deliverable and in section 6 we compare them with the cloud broker system proposed in this document to analyse the expected innovations. The requirements of the cloud brokerage use case are presented in section 7 and this is used in section 8 to propose a high-level design of the cloud broker system. Section 9 provides a summary and conclusion of the work presented in this deliverable.

2.1 Purpose

The main purpose of this Work Package (WP) 6.4 is to demonstrate the implementation of a cloud broker with components derived from the OPTIMIS toolkit as well as augmented by other functional components from outside. The purpose of this deliverable, D6.4.1, is to report the initial work done defining the use case, exploring the requirements and considering an initial design. Specifically this deliverable:

- Introduces the Cloud Brokerage use case scenario
- Explores the business and exploitation cases for the use case
- Identifies the additional requirements presented by the use case
- Presents a high level design of the cloud broker system

2.2 Glossary of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Deliverable</td>
</tr>
<tr>
<td>DoW</td>
<td>Description of Work</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>CB</td>
<td>Cloud Broker</td>
</tr>
<tr>
<td>IP</td>
<td>Infrastructure Provider</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>CAE</td>
<td>Cloud Aggregation Ecosystem</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
</tbody>
</table>
3 Use Case Scenario

The use of cloud based services in order to provide online services to customers is expected to bring in a new era in the area of ICT infrastructure and delivery. In a simplistic scenario, a service provider (SP) decides to host the service it wants to provide to an end customer on the infrastructure provided by an infrastructure provider (IP). This is the current state of art in the use of the cloud services and is considered as a simple scenario because of the limited flexibility available to the SP to split its services into components and deploy them into infrastructures provided by multiple IPs.

However it is expected that the growth and maturity of the cloud offerings would necessitate the building of delivery models that will allow use of multiple IPs for the hosting of multiple components in a single service. It is anticipated that the evolution of such a delivery model would then lead to the formation of a service entity know as the Cloud Broker that provides the SPs, at minimum, with a mechanism to choose a group of IPs from a list of available ones for deploying various components of its service based on various parameters. This Work Package considers the concept of this Cloud Broker in detail.

3.1 Storyboard

The main aim of WP 6.4 is to showcase the use of the OPTIMIS toolkit to build up a cloud services brokerage ecosystem that allows the Service Provider (SP) to use multiple Infrastructure services provided by respective Infrastructure Providers (IPs) by integrating them in a way to as to implement a singular service or process. The aim is to utilize the various components of the toolkit and thus leverage the work done in other work packages of the project. While the initial WP’s Description of work (DoW) describes three scenario setups with varying levels of complexity, in this deliverable we mould the presentation to concentrate on the scenario specific to the cloud broker and use the other two scenarios as stepping stones and stretch goals of the WP.

The Cloud Broker (CB) can be considered as an architectural, business and IT operations model that enables the delivery and management of different cloud services in a framework that provides consistent provisioning, security, administration and other support. In this use case, an SP planning to deploy a service in the cloud approaches a CB with a given set of functional requirements and constraints (including costs, performance etc.) with the aim of selecting the best available match of IPs in terms of the functional requirements as well as other variable constraints like cost, SLA parameters and other non-functional requirements like audit, compliance and security capabilities.

![Figure 1: Cloud Broker ecosystem showing the players involved.](image-url)
The cloud broker will also envisage providing value added services that will help provide a better integration of the SP’s internal IT processes into the IPs. Examples of these include the ability to extend internal identity management systems into the cloud, enforce IT policies both at the perimeter of the SP and also within the various IPs and also performing usage monitoring, reporting etc.

This is a functional as well as complexity-based evolution over the SP’s use of multiple IPs scenario considered earlier in other parts of OPTIMIS, in which the SP combines services provided by multiple IPs to implement and realize a service.

The Cloud Aggregation Ecosystem is considered as a logic evolution of the cloud broker model projected into the Service Oriented Architecture realms, drawing parallels with the concept of Virtual Organisations. The CAE is considered as a “stretch goal” for the WP. This means that the requirements of a CAE will be kept in mind when designing the cloud broker components and even some of these functionalities will be implemented in a mature version of the prototype, it will not be the official deliverable of the WP’s work.

In the CAE scenario, the aim is to aggregate the core business services and management services within the infrastructure and provide the SP with an aggregated ecosystem that can be dynamically extended and administered. This will simplify the dynamic provisioning of cloud infrastructure resources and further add existing monitoring and management services to it from across the different cloud environments. This offers the potential to treat both IT and business functions as a series of interconnected cloud services. CAE offers a means to architect a Service Oriented Infrastructure (SOI) on the cloud that is built on the fusion of:

a) Composition of loosely coupled services based on an evolution of SOA principles applied to services that reside on cloud platforms

b) Distributed management of ICT resources applied on federations of cloud platforms

c) network resource management based on a federated Operational Support System (OSS) architecture built on top of an in-cloud Network as a Service (NaaS) offering.

This scenario adds the capability to incrementally build new service offerings by mixing together reusable functions (common capabilities) provided by off the shelf components and 3rd party cloud platforms in a new offering. More specifically CAE refers to the federation of a set of distributed virtual hosting environments for the execution of an application, integrating value-adding services (VAS) with these hosting environments, and providing a single (logical) access point to this aggregation. From the perspective of the application consumer, these federations are transparent and constitute an integral part of the service being offered.
3.2 Actors Involved in the Use Case

The following actors have been identified from the storyboard description:

- **Service Provider** develops the various components of the service that needs to be deployed.
- **Infrastructure Providers** provide the infrastructure where the service provider could deploy its service components.
- **Cloud Broker** takes in the functional and non-functional requirements from the SP for the various components of its service and performs a match with IPs that can provide compatible cloud service. It could also provide other value-added services to the SP and the IP.
4 Business Case

In this section we present the business case for the work carried out in this WP as an means of providing a commercial justification for the work.

4.1 Analysis of the Market

The use case scenarios presented before are example of how the OPTIMIS toolkit can help on developing cloud services. From the use case definition we have identified the different parties who would be interested in the use case results.

- **Service Providers (SP) & Independent Software Vendors (ISV):** The broker model investigated in this WP and in general the use of OPTIMIS can reduce investments and costs for developing and running their software services. The result of this use case in particular would provide the SPs and ISVs with a means to further minimize the cost of deploying the service by providing best matching services from a list of IPs.

- **Cloud Infrastructure Providers:** The broker functionality allows the IP services to be best matched against the requirements of the PS. This naturally provides best fits between SP and IP and increases the number of targeted customers.

- **Cloud Brokers:** The key player in this model would be able to make use of the results to provide means for the IP and SP to publish service requirements and functionalities and provide a service to find the best match between them. They can earn revenue for this basic service or also provide value added service to the SP to facilitate the deployment of the service.

According to market analysis firm Gartner, the current market for Infrastructure as a Service (IaaS), which is the main focus market for OPTIMIS, is estimated to be US$3.7 billion in 2011 [1]. If generic cloud services are also considered, the market is estimated to be US$68 billion in 2011. However, these numbers are for “vanilla” IaaS and cloud services and our argument is that the result of the work done in this WP can lead to further revenue streams leading to higher actual numbers.

4.2 Expected Market Growth

It is expected that enterprise use of cloud will increase many fold in the coming years. According to Gartner, the market for the IaaS services is expected to grow from the current $3.7 billion to reach $10.5 billion in 2014, while that for a generic cloud market is expected to grow from $68 billion to $148 billion in 2014.

Most current use of cloud services involves scenarios where a single cloud infrastructure/service is used by the enterprise/customer. However, this is expected to change drastically as cloud solutions become more mature and the enterprise starts to use several cloud services (and by extension providers) in their internal IT processes. We foresee that this will then lead to the use of multiple cloud services for a single business process by the enterprise. Examples could include the use of the EC2 IaaS service for less data sensitive virtual application and the use of, say, BT VDC for virtual applications that need certain assurances about environment in which the sensitive data is being used. Both these virtual applications could then be used within the enterprise to, for example, perform modeling simulations. Such collaborative process is already in existence in a drummed down manner, for example, where the Google App Engine environment is used to compute on data that is stored in the Salesforce service [2] and at the Software-as-a-Service level where Facebook was integrated with Salesforce [3].
Analysts have been looking at cloud broker services as a part of the “on-ramps” services [4]. Vendors that fall into this category generally provide templates for commonly used cloud server and application configurations, or more advanced offerings with more robust management capabilities and customization options. According to [4] on-ramps are the second-largest cloud management segment, representing the 24% of the total revenue generated by cloud management providers (2009). Revenue generated by on-ramps totaled $14m in 2009 and is expected to grow at a CAGR of 66% to reach $108m in 2013. It needs to be however noted that on-ramps haven’t been offering the ability to pass workloads between IaaS and PaaS platforms or between cloud vendors. Given OPTIMIS intent to provide such a capability, the overall market is expected to grow materially.

According to analysts, the cloud broker model is the next phase in the process of cloud market maturity. The top-end of the cloud revenue projected by analysts can be realised only by the use of such mature technologies and service models. Such delivery models are expected to help service providers improve the economics of delivering cloud-based services and thus making them more appealing to customers. In addition to simple QoS/SLA-based matching service, the cloud broker can provide other value-added benefits like preventing vendor lock-in, providing compliance and audit services, assurance, transparency and security. There exists a separate market for these services that can also be exploited by the cloud broker model. In recent times a few players have made services available that mirrors some of the functionalities we expect from the CB [5]. However, such services do not cover the full expanse of service envisaged from the OPTIMIS CB service. Nevertheless there is evidence that some of the infrastructure and other cloud service companies are interested in acting like a broker of cloud management tools and enable service providers and enterprises with these value-added services.

Since the CAE is an advanced form of service delivery and in some ways is ahead of the curve in terms of conceptual models, it is harder to get an analysis of the demand for it. In some ways, it is one of the various models being referred to in the ‘The Future of Cloud Computing’ report [6], “Cloud technologies and models have not yet reached their full potential and many of the capabilities associated with Clouds are not yet developed and researched into a degree that allows their exploitation to a full degree”.

### 4.3 Exploitation Plan

WP 6.4 will provide a proof of concept implementation and demonstration of the cloud broker ecosystem, exploiting the OPTIMIS toolkit functionalities to the utmost. Where gaps are identified, the WP will also engage with tools that provide complimentary functionalities, thereby providing a best mix of using results of the project and also existing commercial or other tools and services.

The multi-cloud scenario is already being implemented by select cloud providers. However, these existing offerings are static partnerships between cloud providers and do not put the service providers (SPs), who are the end customers of the cloud services, in charge. We foresee the multi-cloud scenario as described above being exploited by the SPs to enable dynamic IT process fulfillments using multiple IPs. This will enable the SP to onboard more process into the cloud in a flexible manner. In particular, the components like the SDO can be used by the SP to power such a scenario in a seamless manner. The IPs can also use the effort and result of this scenario to implement mechanisms that will help setup the multi-cloud business model.

We foresee the cloud broker scenario being exploited by the larger IP to carve out a larger role for itself within the cloud ecosystem. This scenario is also important to those players who want to provide just a cloud broker service to the customers. These entities would have no
infrastructure to provide by themselves and would be devoted to providing the broker service using the cloud services provided by other dedicated IPs. In recent times, while some companies have started making services available that aim to fulfill the CB role, we see the OPTIMIS CB as being more comprehensive solution that takes into account issues like Cost, Trust, Risk and Ecosystem factors when making the choices as well as provide the SP will more seamless mechanisms to on-board their services into the cloud. The IPs interested in becoming part of the CB-based ecosystem can do so by implementing the various tools provided by the OPTIMIS toolkit that makes aspects of providing the service easier, manageable and more scalable.

The output from CAE can be exploited by existing service providers within the cloud ecosystem as well as by companies that are providing core and value add services to a typical IT infrastructure. The management framework that is expected to be produced by the WP for powering the CAE can be used by existing (possibly existing IPs) or new players in the cloud service ecosystem to build a service that provides the underlying setup for a CAE overlay. Existing IPs can use the common capabilities provided by OPTIMIS toolkit optimized for the CAE scenario to augment their existing capabilities to make them compatible with the needed of a CAE system.
5 State of the Art

The current state of arts falls mainly into two categories – use of multi-cloud and primitive work on cloud broker service.

The concept of using multiple cloud provider services as a means to power an IT process is not unique and has been attempted with initial success in the current market. The use of data stored in Salesforce service by Google App Engine environment [1] as well as the integration between Facebook and Salesforce by a Facebook application [2] are examples of such services. However, all these examples have been static collaborations and furthermore, in the case of Salesforce-AppEngine example the collaboration was defined and brought out by the cloud service providers at their side and not initiated by the SP/customer and in the case of the Facebook-Salesforce example, there is no specific SLA, cost, risk, trust or other variable based choices made available to the application writer.

The cloud broker concepts, as explained earlier, is in its infancy and while some attempts have been made to create services that resemble that of a cloud broker, they are rudimentary in nature. A Gartner report [7] divides the “Cloud Service Broker” business into three:

- Cloud Service Intermediation: offer intermediation for multiple services to add value-adds like identity management or access management.
- Aggregation: A relatively fixed aggregation of multiple cloud services into one or more new services.
- Cloud Service Arbitrage: a more dynamic version of aggregation which aims to provide flexibility and opportunistic choices for the service aggregator

The functionalities identified for the Cloud Broker in OPTIMIS mirrors that defined by Gartner above.

A set of products and services that provide functionalities that overlap with the service broker is that of the “gateway”. The Vordel “Cloud Service Broker” service (in invitation-only beta) is an example of this service. It provides a mechanism “for securely integrating local on-site applications with offsite cloud service key value-added services and enabling monitoring, management and policy enforcement for all transactions.” [8] What this boils down to in features is that the software allows a seamless integration of multiple cloud service provider’s services into the existing internal enterprise setup allowing for cleaner management of the connections, including API Keys that are required for authentication. This gateway functionality is expected to be an integral enabler of the cloud broker architecture.

Cloudswitch [9] is another product which provides comparable services. It advertises itself as a “the enterprise gateway to the cloud” and provides the ability to seamlessly provision new virtual machines (VMs) or move existing ones into Amazon and Terramark cloud infrastructures. While the product provides a good set of features for acting as a gateway between the enterprise’s local data centre and the cloud, it does not really provide any of three functionalities identified by Gartner.

The JamCracker system, for example, provides a platform where it “aggregates and distributes on-demand services through a global ecosystem of Service Providers, Resellers, System Integrators, and ISVs” [5] but the service is largely limited to providing this aggregation system and some value-adding services. It does not provide a proper brokerage service whereby an entity looks at the actual QoS requirements of the service under question, the various IPs that could potentially meet them, rank them against parameters like cost, trust, eco-efficiency, risk etc. and provide functionality to on-board these applications in to the various IPs finally selected.
The CAE model has so far not been explored in the cloud industry. The nearest similar system that one can consider is the Service Oriented Architecture (SOA) concept of Virtual Organisation where multiple business processes are brought together in a loosely coupled manner to provide a customer with a consolidated way to outsource an IT process. While the concept is similar to that of the CAE, our view is that the use of cloud based services, especially IPs, provides a big difference in the players involved that the assumptions and functionalities of the system design would drastically differ.
6 Expected Innovation

As described in the previous section, the current solutions fall short of the cloud brokerage model that we envisage as end result of the work performed in this Work Package. Based on the existing solutions, we expect the work in this WP to bring out the following innovations:

- Matching of requirements and functionalities: The WP aims to provide standards-based SLA negotiation and agreement mechanisms to allow the broker to perform a match between the requirements of the SP and the functionalities provided by the various IPs. This is something that is lacking in the current offerings and form the core of the broker functionality.

- TREC based decision making: The OPTIMIS toolkit provides means to make decision on which IP and SP to engage with based on Trust, Risk, Eco-efficiency and Cost parameters. The use of this functionality allows the broker to make SP-IP matches based on TREC parameters. While the use of cost parameter might be an obvious functionality, the other three parameters add a new level of options to the scenario.

- Value-added services: The WP aims to showcase the ability of the cloud broker to provide value-added services to the SP (and maybe even the IP), making it easier for the parties involved to move the services and offer their services in the cloud. For example the ability to enforce corporate IT policies in the cloud environment as effectively as in a corporate data centre is a much sought after capability, along with seamless identity management capability and the broker is in an advantageous position to provide some of these capabilities.

- Federation capabilities: In the current offerings, the IP is able to leverage only on its dedicated infrastructure resources to provide a service to the SP. However the OPTIMIS toolkit allows the IP to internally use the services of (federate to) other IPs to cope with scaling demands. This capability can be brought into the brokerage scenario, allowing for a more efficient and resilient working of the IPs.
7 Requirements Analysis

As a part of the design process, WP 6.4 undertook a requirements analysis of the Cloud Broker system and contrasted it against that of the general OPTIMIS toolkit. In this section we present the main requirements that were identified as being above and beyond that of the OPTIMIS toolkit and components, as identified by deliverable D 1.1.1.1.

In order to have a basic understanding about the difference between the four use cases considered in other OPTIMIS WPs - namely private cloud use, cloud bursting use, cloud federation and multi-cloud, and the ones considered in WP 6.4, we also carried out an analysis of the risk assessment tool. The results of this exercise are provided in Annex B.

7.1 Identified functional requirements

7.1.1 SP using Multi-cloud services

Assumptions:
The following assumptions are made about the working of this use case.

1. The algorithm of the TREC components is completely automated and the SP makes its decisions purely based on the service requirements in Manifest file. There is no adhoc reasoning involved.

2. A service will have multiple components (that maps to one VM type/image) to be deployed, either at multiple IPs or at the same IP.

Generic requirements

1. SLA has to be negotiated and established specific to each of these components.

2. A component-specific (and not service specific) TREC assessment needs to be performed to know which IP is best for which component.

3. SP should be able to decompose the manifest of a full service to multiple component-level manifests since this is the granularity being considered in the multi-cloud scenario.

Trust Requirements

1. The capability to get the Trust levels of a group of IPs. This ensures that the SP using multi-cloud service gets all the IPs with high Trust and gets the best combination for its service to be deployed.

2. The Trust component must have the capability to identify the best combination of IPs needed by the various components and rank the combinations based on their Trust Level. It should consider the influence that choice of one IP has on the trust calculation of another (if there is any).

Security Requirements

1. The Service Integration Layer needs the Identity management and integration capabilities to consolidate the identities and authentication capabilities that might be different across the participating IPs.
2. A simplified key management system or keystore functionality many be required to handle the multiple IP access keys and other public and private keys as needed or generated.

3. Access management system is required to integrate access rights across multiple IPs

4. Secure (secret, verifiable and authenticated) communication capabilities are required between the Enterprise and the multiple IPs

5. Overlay network capabilities are required for integrating between service components spread across IPs and even also between the service components and SP’s network

Risk

1. The influence of the choice of an IP on the risk profile of another IP for a different component needs to be considered.

Cost

1. The overall cost assessment is required for the group of IP’s selected.

Service Deployment Optimiser

1. The SDO is required to have the capability to manage the cloud services across multiple IPs

2. The SDO needs the capability to interact with Admission control of different IPs to deploy its service.

3. The SDO needs the capability to interact with data management of different IPs to upload, download and delete data.

Service Manager

1. The Service manager needs to capability to deploy its service at multiple IPs

2. The Service manager needs to capability to un-deploy its service at multiple IPs

7.1.2 SP using Broker

It is to be noted that the requirements identified below is on top of the general requirements identified in ID1.1.1.1 for OPTIMIS in general and also builds on the requirements identified for the multi-cloud scenario above.

Trust Requirements

1. SP provides all the functional and non-functional requirements to the Broker. The Broker must have the capability to find either a single IP or a combination of IPs to fulfill the requirements of the SP.

2. In the case where the broker may need more than one IP to fulfill the requirements of the enterprise, it must have the capability to partition all the requirements and get the Trust levels of IPs based on sub-requirements. This helps the broker to select the most Trustworthy IPs.
3. The Trust component must have the capability to identify the best combination of IPs and rank the combinations based on their trust level.

4. The Trust component of the SP should also be able to assess the Trust level of the Broker

**Security Requirements**

1. The Identity management solution at the broker should manage and map the identities between the SP and IPs and also provide context to the federated identities.

2. In order to allow the SP to upload the VMs to individual IP repositories, the Broker will have to provide a means to delegate access of these IP-based repositories to the SP.

3. Secure communication and management/administration middleware will be required between the SP and the Broker and also between the Broker and the multiple IPs.

4. Overlay network capabilities should be provided by the broker so that the enterprise can integrate its network with the VMs it is using on the IPs’ networks.

5. A Key Management System will be required to manage the IP access keys, PKI keys as well as other security tokens as needed or generated by the Identity and Access management systems.

**Other Requirements**

1. The broker may need the capabilities to negotiate and establish SLAs with the different Cloud providers based on the partial requirements (from decomposed manifest file) of the SP’s SLA.

2. As in the case of SP in the other use cases, the Broker needs monitoring capability for example: SLA violations, VM performance etc.

**General Requirements**

1. The SP needs a mechanism to upload the manifest and VMs to the Broker (This is with the assumption that all the communication between SP and IP passes through the Broker).

2. A component needs to be responsible for getting the individual TREC assessment results from each of the TREC components (such as Trust, Risk, Eco-efficiency and Cost) and combine them to get an overall assessment result. This could be the SDO of the current architecture.

3. If multiple brokers are considered, a means of selecting the best broker needs to be architected, possibly based on the TREC assessments. Since the properties of a broker may differ from that of an IP, the selection of broker may differ from the existing mechanism of selecting IP.

4. Once the VMs are deployed, the broker would receive the IPs of different VMs. These IP addresses need to be forwarded to the SP for administration functionalities.

5. The Broker needs the capabilities to decompose the manifest of a service provided by the SP to multiple sub-manifests, specific to each service components deployed at the different IPs.

**Assumptions**
1. The algorithm of the TREC is completely automatic and the Broker is able to make decisions purely based on the Manifest.

7.2 Gap Analysis

The requirements analysis performed in the previous subsection can also be considered as output of a gap analysis exercise since the requirements identified are on top of the requirements that have already been identified for the OPTIMIS toolkit and components in D 1.1.1.1. Thus the requirements identified in this document are those that have not been implemented in the current version of the OPTIMIS toolkit and the components that make it.
8 High-level Design

In this section we provide a high-level design of the cloud broker, keeping in mind the use case scenario and the functional requirements identified in earlier sections.

At an abstract level we plan to employee a services integration layer that uses well-defined interfaces and standardized calls between different pre-selected Infrastructure Providers (IPs) resources to provide the loosely-coupled integration required for the completion of the enterprise’s process. We will examine the generic requirements of such a process composition from the enterprise’s view point and the necessary technical resources necessary to realise such an orchestration. From the point of view of the cloud service providers, we will investigate the extra capabilities that need to be exposed to enable the enterprise to tie together the full orchestration requirements. This includes the common requirements such as trust establishment, identity management; Web Service based API calls for accessing the data etc.

As identified from the original OPTIMIS requirements as well as the additional ones in this document, the CB needs to have the capability to, among others:

- Effectively match the requirements of the SP with the service provided by the IPs.
- Negotiate with SPs and IPs over service level agreements.
- Effectively deploy services of SP onto the IPs.
- Maintain performance check on these SLA's and take actions against SLA violations.
- Ensure data confidentiality and integrity of SP’s service.
- Enforce access control decisions uniformly across multiple IPs.
- Securely map identity and access management systems of the IPs and SPs.
- Analyse risks and take appropriate actions against them.
- Manage the control APIs of IPs so as to provide uniform schema to the SP-level users.

On the basis of the requirements and capabilities identified, the functional components needed at the CB’s platform can be categorized as shown in figure below
The functional components needed by the broker to provide these broker capabilities are specified in Figure 3 above.

The **API Manager** is a mechanism through which consumers can interact with the cloud broker for performing cloud related actions including creating and managing cloud resources like compute and storage components. It is also in charge of interfacing with various interfaces exposed by the IPs, including non-OPTIMIS IPs. The **Deployment Service** unit handles the deployment of services which cloud provider offers to the service consumer. To exemplify, through this unit the broker requests the cloud provider to start a virtual machine which the consumer can use for compute purpose or to create a storage space for user’s data.

The **Staging Service** unit is to handle cloud burst and spill over situations. Since Cloud services are offered on pay-as-you-go basis, and are highly scalable, service consumers can demand extra resources and the broker need to ensure that a suitable cloud provider is in place to handle the request. The broker interacts with the respective cloud provider on which service consumer’s applications and data are currently residing in a proactive manner to demand more resources. In case the cloud provider cannot meet the demand for the extra resources, the staging and pooling unit will find out another suitable match from the pool of underlying cloud providers and request the resource.

**Identity and Access Management** unit is a vital unit as it not only verifies its own employees but also keeps record of all the service consumers - required enterprise details, assigned cloud providers, type of service like storage or compute and classification criteria. The classification criteria is decided during the SLA negotiation phase between the broker and the consumer and based on it, broker grants access to the employees of the consumer enterprise. As will be seen later on, the enterprise’s cloud management entity forwards a storage or compute request to the broker on behalf of its employee along with the classification criteria. Identity and access management unit then generates a one-time token on the basis of assigned classification criteria.
The **SLA monitoring** unit constantly monitors all the SLAs negotiated by the SLA management unit. It checks to see if there are any impending SLA violations and if any, to take the specified preventive measures. The **Capability Management** unit keeps tab of all the capabilities provided by the various providers like its delivery and deployment model, security mechanism, fee structure, IT functionalities and all other necessary details. Whenever a service consumer approaches the broker for cloud services, this unit matches the consumer’s functional and SLA requirements with the services each cloud provider offer and finds the most appropriate and suitable match. This unit is also referred by the staging and pooling unit during sudden spike in demand of storage space. The **Audit** Unit periodically audits broker’s platform as much as possible using capabilities provided by the cloud provider. Audit is performed to ascertain the validity and reliability of information and to provide an assessment of internal controls. A similar functionality is provided from compliance perspective by the **Compliance** unit. Gateway **Firewall** provides perimeter security to the broker system by blocking malicious traffic to and from the various components exposed by the interfaces of the cloud broker service.

In addition to the firewall module, the **Platform Security** unit manages the overall security of the broker’s platform. Provisions and policies are adopted to prevent unauthorized access, misuse, modification or denial of network or network accessible resources. It provides a protection at the boundaries of the platform by keeping out intruders. Furthermore, the intrusion detection system which is a part of this unit focuses on protecting data from malware, virus, worms, or trojans.

The **Usage Monitoring** unit monitors the usage of the services by the cloud consumer, and generates monthly bills for them. The **SLA Management** module controls all the SLAs in place between the broker and consumer.

Given this design, an exercise was carried out to determine the match between the OPTIMIS toolkit capabilities, the components that provide those capabilities and the broker’s design components. The table below summarises the result of the findings.

<table>
<thead>
<tr>
<th>Design Components</th>
<th>OPTIMIS Toolkit match</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Manager</td>
<td>None. Capability need to be added</td>
</tr>
<tr>
<td>Deployment Service</td>
<td>Service Manager</td>
</tr>
<tr>
<td>Staging Service</td>
<td>Partially met by the Elasticity Engine</td>
</tr>
<tr>
<td>IdAM</td>
<td>Security services</td>
</tr>
<tr>
<td>Capability Management</td>
<td>Service Deployment Optimiser</td>
</tr>
<tr>
<td>Platform Security</td>
<td>Partially met by the security services</td>
</tr>
<tr>
<td>Audit</td>
<td>None. Capability need to be added, most likely to the security services</td>
</tr>
<tr>
<td>Compliance</td>
<td>None. Capability need to be added, most likely to the security services</td>
</tr>
<tr>
<td>Gateway firewalls</td>
<td>None. Capability need to be added, most likely to the security services</td>
</tr>
<tr>
<td>SLA Monitoring</td>
<td>SLA Management</td>
</tr>
<tr>
<td>SLA Management</td>
<td>SLA Management</td>
</tr>
<tr>
<td>Usage Monitoring</td>
<td>Monitoring</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>

*Table 1: Comparison of Broker components and OPTIMIS Toolkit components*
9 Conclusion

In this deliverable we report the work performed in the first six months of the WP 6.4 as part of the Integration and Experimentation activity. In particular it looks at the business case and exploitation plan around the Cloud Broker use case and identifies the additional requirements associated with it before proposing a high-level design of the broker platform.

The next steps to be carried out in this work package would involve refinement of the architecture to encompass lower level details and to implement a prototype of the system.
10 References

[1] "Gartner Maps Out the Rapidly Evolving Market for Cloud Infrastructure as a Service"  
http://www.gartner.com/it/page.jsp?id=1622514

[2] "Salesforce and Google App Engine"  
http://thoughtsonsalesforce.com/blog/salesforce/crm/73


[8] "Vordel Cloud Service Broker Invitational Program"  
http://www.vordel.com/products/cloud_service_broker/beta.html

Annex A. License conditions.

This is a public deliverable that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons http://www.creativecommons.org

This license allows you to

to copy, distribute, display, and perform the work

to make commercial use of the work

Under the following conditions:

1. **Attribution.** You must attribute the work by indicating that this work originated from the IST-OPTIMIS project and has been partially funded by the European Commission under contract number IST - 257115

2. **No Derivative Works.** You may not alter, transform, or build upon this work without explicit permission of the consortium

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

This is a human-readable summary of the Legal Code below:

**License**

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE (“CCPL” OR “LICENSE”). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

**"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

**"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purposes of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

**"Licensor"** means all partners of the OPTIMIS consortium that have participated in the production of this text.

**"Original Author"** means the individual or entity who created the Work.

**"Work"** means the copyrightable work of authorship offered under the terms of this License.

**"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

   to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

   to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

For the avoidance of doubt, where the work is a musical composition:

**Performance Royalties Under Blanket Licenses.** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

**Mechanical Rights and Statutory Royalties.** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and
distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

**Webcasting Rights and Statutory Royalties.** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved.

**4. Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

**5. Representations, Warranties and Disclaimer.** UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

**6. Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**7. Termination**

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

**8. Miscellaneous**

Each time You distribute or publicly digitally perform the Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.
Annex B.  Risk Assessment Analysis

This Annex summarises the requirements for each of the different use cases in terms of the risk assessment tools. The first four use cases are taken from OPTIMIS and at the end are the three use cases for WP6.4. As such we are trying to see whether there is similarity among the use cases in terms of risk assessment.

B.1  Original OPTIMIS use cases

B.1.1  Use case: Private Cloud

Figure 4: Component Interaction for risk assessment in private cloud

At SP level:

The risk assessment here interacts with the SDO. It assesses the risk with working with the IP and sends a list of IPs back to the SDO presented as ranks or preference of working with them.

At IP level:

During the deployment phase the risk assessor interacts with CO and Cloud QoS to assess the SP on whether to work with them. At runtime the IPRA will be querying data periodically from the monitoring database. If something happens it will communicate mitigation strategy back to VM manager and CO. It will be their decisions with mitigation strategy to implement.
B.1.2 Use case: Cloud Bursting

Cloud bursting scenario is when one IP will burst its work onto another IP. Most of the interactions are the same as the private cloud.

**At SP level:**
Same as private cloud risk assessor.

**At IP level:**
Similar to private cloud risk assessment at IP level. However additionally the Risk assessor will include mitigation strategies which may suggest bursting to another IP. Then the CO (at IP1) can make decisions to burst or not.

If it does decide to burst it needs to talk to a SDO within itself to access the available IPs and create a ranking of IPs after assessing the risk of working with them. After making the decision, the IP2 will do risk assessment same as private cloud risk assessment at IP level.
B.1.3 Use case: Federated Cloud

In a federation of cloud, there is no need to do preassessment between the IPs when requested to burst. This is because they all belong to the same domain, thus there will be no risk assessment when IP1 decides to burst.

The risk assessment is similar to the ones at the IP level in cloud bursting, but there is an additional communication between the risk assessors at the IPs in order to update the information on the performance of services. This allows all risk assessors to be aware of the situation in a federation of clouds.

B.1.4 Use case: Multi-Cloud

Multi-cloud scenario is very similar to cloud bursting scenario. However in a multi-cloud bursting the cloud would burst more than one time depending on the service. Each time it bursts it needs to perform pre-assessment on IP calling its service.
Risk assessment will be exactly same as cloud bursting.

**B.1.5 Use case: Enterprise using multiple cloud service providers**

Risk assessment will be similar to OPTIMIS multicloud scenarios.

**B.1.6 Use case: Enterprise Cloud Broker**

Risk assessment will be similar to OPTIMIS multicloud scenarios. The only difference with the use case above here is that the TREC tools are separated outside and can make decisions itself.

**B.1.7 Use case: Cloud aggregation Ecosystem (CAE)**

Risk assessment for federated cloud setup can use the risk assessment from the SP level, where the SP tries to assess the risk of working with the particular IP. Is the enterprise client similar to an SP in the above use cases?