Common Capabilities for Service Oriented Infrastructures In A Grid & Cloud Computing

Prof. R.T Nakhate
Nagpur University DMIETR, Salod Wardha

Prof. M. Sayankar
Nagpur University BDCOE Sevagram, Wardha

Abstract-- The aim of the Business Experiments (BE) in GRID project was to generate knowledge, technological improvements, business demonstrators and reference case studies to help companies and other organizations to establish effective routes to foster the adoption of Grid and Cloud Computing, which are often summarized under the term Service Oriented Infrastructures (SOI)1, and to stimulate research to help realize innovative business models using these technologies In terms of technology innovation, the BEinGRID team has analyzed and classified the technical issues involved and the generic solutions developed by and for the Business Experiments (BE).

Index Terms— Data, Security, Cloud, Disk, VM,SLA ,Grid.

I. INTRODUCTION

The required common capabilities have been categorized in the following thematic areas:

1. Capabilities for Life-cycle management of Virtual Organizations help businesses establish secure, accountabl and efficient collaborations sharing services, resources and information. These include innovations that enable the secure federation of autonomous administrative domains, and the composition of services hosted by different enterprises or in-cloud platforms.
2. Trust & Security capabilities address areas where a perceived or actual lack of security appears to inhabit commercial adoption of SOI. These include solutions for brokering identities and entitlements across enterprises, managing access to shared resources, analyzing and reacting to security events in a distributed infrastructure, securing multi-tenancy hosting, and securing the management of in-cloud services and platforms. These innovations underpin capabilities offered in Virtual Organization Management and other categories.
3. Software License Management capabilities are essential for enabling the adoption of Pay-As-You-Go (PAYG) and other emerging business models, and had so far been lacking in the majority of SOI technologies including Grid and Cloud computing.
4. Innovations to improve the management of Service Level Agreements cover the whole range from improvements to open standard schemes for specifying agreements, to ensuring fine-grained monitoring of usage, performance and resource utilization.
5. Data Management capabilities enable better storage, access, translation and integration of data. Innovations include capabilities for aggregating heterogeneous data sources in virtual data-stores and ensuring seamless access to heterogeneous geographically distributed data sources.
6. Innovations in Grid Portals enable scalable solutions based on emerging Web2.0 technologies that provide an intuitive and generic instrumentation layer for managing user communities, complex processes and data in SOI.

II. LIFE-CYCLE MANAGEMENT OF VIRTUAL ORGANIZATIONS

1. The identification and selection of business partners (based on their reputation and the suitability of services that they offer) among an available pool of service providers or consumers.
2. The creation and management of a Circle-of-Trust among the selected partners.

The "VO Set-up" common capability offers a standards-based foundation for business solutions to these problems. This capability facilitates the identification and selection of business partners engaging in B2B collaborations, the creation of a distinct context for each of these collaborations, the creation and lifecycle management of a distinct Circle-of-Trust amongst the business partners involved in each collaboration, and the binding of each collaboration context with the corresponding Circle-of-Trust.

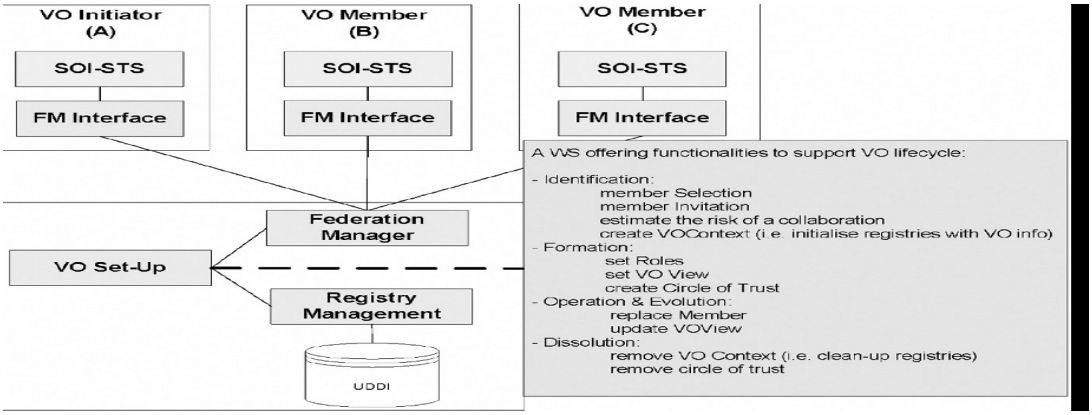

Fig. 2 The high-level architecture of the "VO Set-Up" Common Capability

The following list summarizes some of the most significant improvements achieved by this architecture:

1. It can manage participation in multiple, distinct and co-evolving B2B collaborations.
2. For each B2B collaboration context, the trust relationships between the (identity brokers of) business partners reflect the structure of the value network of this collaboration.
3. It enables evaluating the risk associated with a collaboration based on trust in each participant. In its current implementation, the risk is estimated by evaluating a weighted mean of "reliability" values associated to each member.

III. TRUST & SECURITY CAPABILITIES

The need for security for agile business operations is so strong that, according to Gartner (2009), despite the worldwide economic crisis – or possibly because of it – security aspects such as Identity and Access Management (IAM) remain a critical investment for enterprises of all sizes and market sectors. Through increasing business-level visibility led by data-breach headlines, security spendings continue to rise and take a growing share of overall IT spending. Indeed, IAM alone represents a growing market which accounted for almost $3 billion in revenue for 2006 (Gartner 2009). According to Forrester (2009), security initiatives will focus on: (a) protecting data, (b) streamlining costly or manually intensive tasks, (c) providing security for an evolving IT infrastructure, and (d) understanding and properly managing IT risks within a more comprehensive enterprise framework.
In order to achieve agility of the enterprise and shorten concept-to-market timescales for new products and services, IT and communication service providers and their corporate customers alike increasingly interconnect applications and exchange
data in a Service Oriented Architecture (SOA).

The way businesses interact is therefore evolving, to:

- A work environment that becomes pervasive with a mobile workforce
- Outsourced Data Centers and in-cloud services
- Integrated business process with customers and suppliers across value chains The key security challenges come from this evolution of the way businesses interact, include:
- Business process integration with customers and suppliers across value chains
- Many sources of identity and policy enforced over shared IT infrastructure
- Manage access to resources in environments that are not under one's control

• Ensure accountability over a mixed control infrastructure
• Collect evidence about policy compliance for diverse regulatory frameworks
• Deperimeterisation of corporate ICT while maintaining acceptable levels of
security in business operations

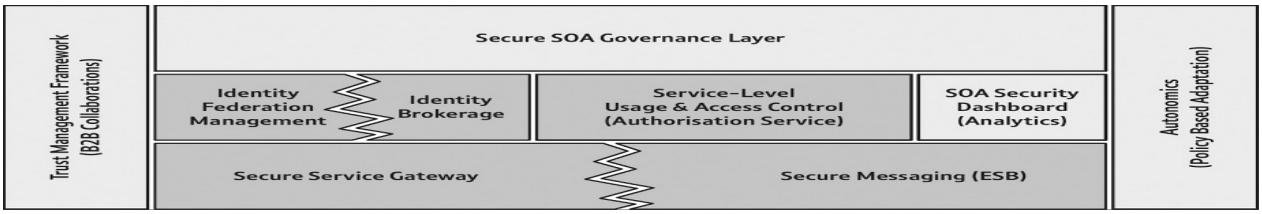

Fig. 3.1 Overview of the security capabilities required by service-oriented enterprises

I.1 Federated Identity Management

1. *Identity Brokerage and Identity Federation Context Management*

This is a capability enabling identity federation and brokerage across business partners.
Early developments of this capability stemmed from collaborative research between BT and the European Microsoft Innovation Centre in the TrustCoM project
[5] It is a customizable platform for Identity-as-a-Service (IDaaS) provision with technological innovations that resulted in the following differentiators compared to what is currently available in the market:

• The business logic of the Identity Broker can be optimized for each identity federation context. This innovation enables the application of different authentication procedures, different federated identity standards, attribute types and entitlements on the same user or resource depending on the purpose of a B2B interaction and the scope of the identity federation. The Identity Broker is therefore configured to compose security primitives in a behaviorally distinct instance of a Security Token Service (STS) optimized for the specific context.
• Administrators can author declarative policies to control information disclosure within the scope of each identity federation. Users can also author policies to control disclosure of user-provided data. In effect, different policies may apply on the same personal data used for different purposes in the same scope or used in different identity federations.
• The Identity Broker has been designed with compliance in mind. An innovative policy issuance mechanism allows associating an administrator's identity with the digital signature of a policy fragment (or a user's identity with digital signatures of user-generated data). It also facilitates providing evidence that policy fulfillment and disclosure of identity data is in compliance with explicitly
defined rules of use.
• This capability has been designed for use within Virtual Organizations (VO). It is easy to manage in multi-administrative environments and integrates
with related VO capabilities For each identity federation context, it represents a partner-specific viewpoint of the associated Circle-of-Trust in a way that trust relationships between Identity Brokers respect supply relationships associated with the domain.
• Finally, it is designed for the in-cloud use – it is equipped with a secure web services remote management interface that enables it to be assembled and managed remotely and provides the basis for an instrumentation layer utilized by collaboration services

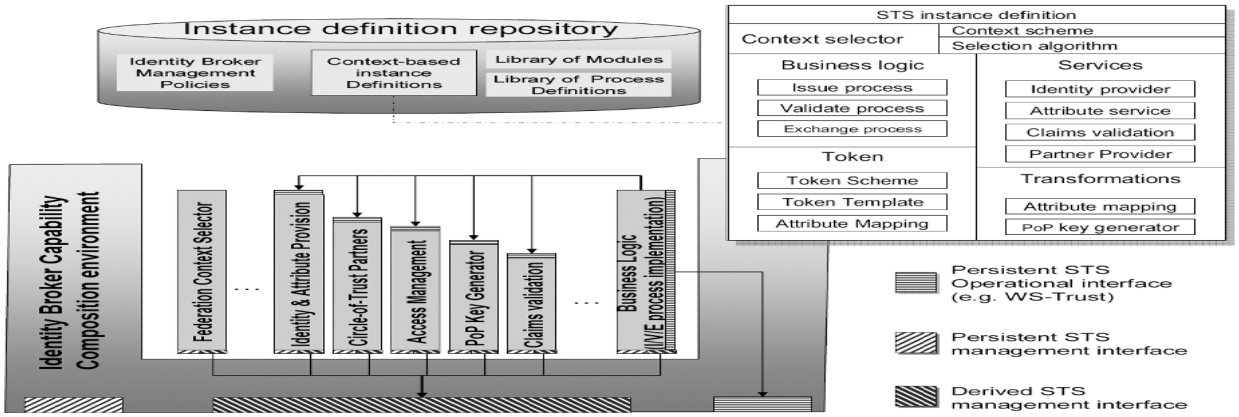

Fig. 3.2 Overview of the Identity Broker architecture

2. *Managing Trust Relationships Among Federated Identity Brokers*

Relationships between federated identity brokers form a trust network can reflect the service-consumer relationships for a particular value network and a particular context. Brokers can share the same federation context identifier (i.e., a shared state reference) and associate it with their internal view of the circle-of-trust that reflects their own trust relationships (i.e., local state). The latter may include assertions recognizing the authority of those identity brokers they trust in this federation context[4]. Directed binary trust relationships can be defined between an identity broker and each of the trusted identity brokers with which it is associated in a federation
context by having the corresponding identity brokers accept these recognition of authority assertions.

I.2 *Distributed Access Management*

Distributed access control and authorization services allow groups of service-level access policies to be enforced in a multi-administrative environment while ensuring regulatory compliance, accountability and auditing.

This access management capability also caters for policies addressing complementary concerns (operational and management) in a multi-administrative environment (see fig. 3.3). It supports policies about the following:

• Subjects access resources in a context, i.e. who can do what on which resource and in which context. These policies are issued (and signed) by administrators authorized to manage resources.

• Constraints on who can author policies access policies, such as the above, or on who can delegate which access rights about which resources in what context.

• Obligations that instruct associated policy enforcement points.

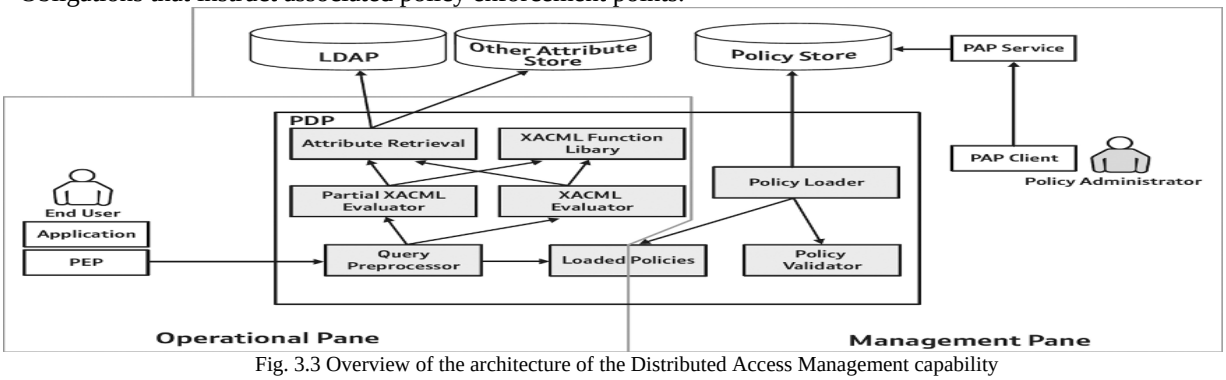

Fig. 3.3 Overview of the architecture of the Distributed Access Management capability

IV. COMMON CAPABILITIES FOR MANAGING SOFTWARE LICENSES

Technological innovation on how software licenses are provisioned and managed throughout the service life-cycle is necessary for enabling commercial applications from independent software vendors (ISVs) on SOI and Cloud

Computing environments. As explained in [5] small and medium sized enterprises (SME) especially from the engineering community stand to profit from this.

The LMA capability is generic, independent of specific middleware choice, and features cost-unit based accounting. It enables using licensed ISV applications in HPC utility or Cloud platforms in a wide range of provisioning scenarios. In combination

with secure access to the license server, LMA facilitates the non-interruptive business transition to pay-per-use models while supporting the current legacy technology that used to manage software licenses. It therefore enables increasing of the market size in the area of SOI and on-demand Cloud Computing.

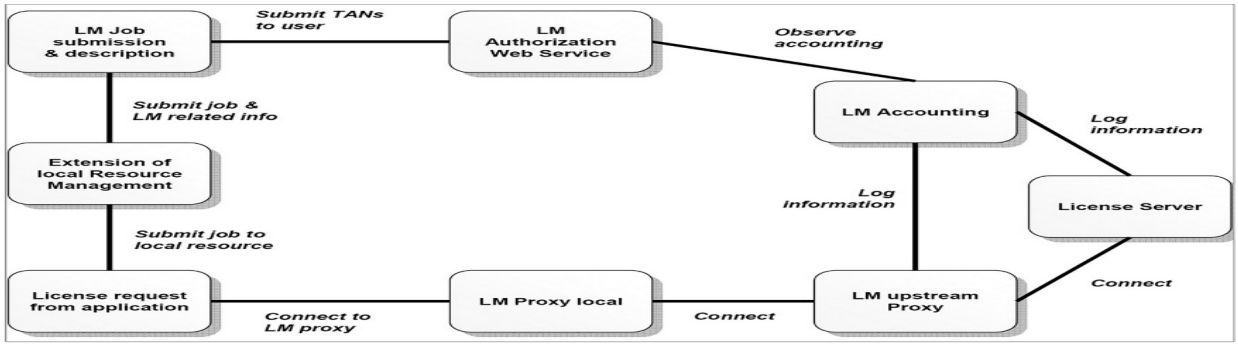

Fig. 4 Overview of the architecture of the License Management capability

V. COMMON CAPABILITIES FOR MANAGING SERVICE LEVEL AGREEMENTS

Quality of Service (QoS) is in essence about a set of quality metrics that have to be achieved during the service provision. These metrics must be measurable and constitute (part of) a description of what a service can offer. The QoS of IT services is often expressed in terms of capacity, latency, bandwidth, number of served requests, number of incidences, etc. The QoS of services offered to the customer is sometimes expressed as a package (for example bronze, silver, gold) and in relation to key performance indicators (KPI). In this case, a match between the elements of the scale and measurable metrics relative to the service is provided.

A Service Level Agreement (SLA) defines the QoS of the services offered. Typically SLA is a formal written agreement made between two parties: the service provider and the service user, defining the delivery of the service itself. The document can be quite complex, and sometimes underpins a formal contract. These define a specific level of service, support options, incentive awards for service levels exceeded and/or penalty provisions for services not provided, etc. Some organizations, attempting to avoid negative connotations, prefer to use the terms SLE (service-level expectation) or SLG (service level goal) for the definition of the QoS of the services they offer.

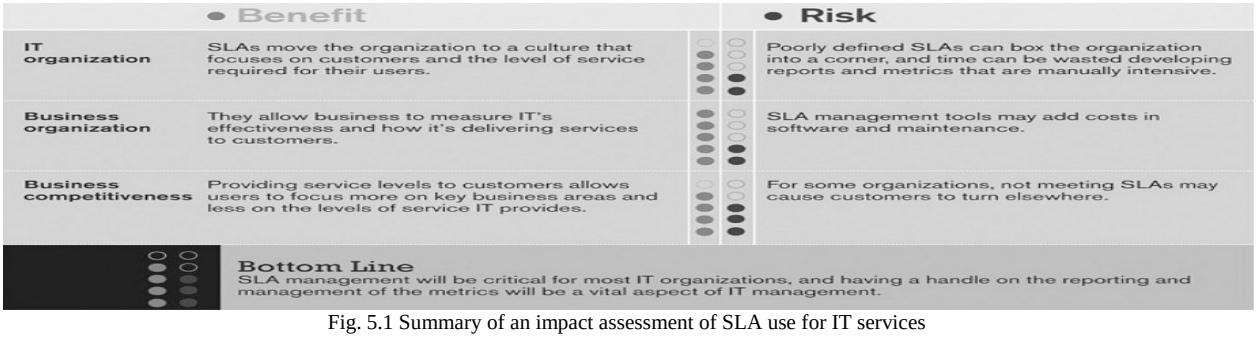

Fig. 5.1 Summary of an impact assessment of SLA use for IT services

A successful SLA strategy must include the ability to collect configuration information on network and server assets, access customer information for business impact analysis, and provide data on all internal or external SLAs[5]. Ensuring that users have visibility of what services IT makes available, what level of service is provided, and that they have the ability to verify the level of service offered can help increase customer satisfaction and improve the overall relationship between IT

and the users. A service-centric approach to SLA management is the cornerstone of a user-centric approach to the IT offered.

Fig. 5.2 Common capabilities for SLA management against the life-cycle of managing SLAs

VI. Common Capabilities for Data Management

Companies in most vertical market sectors that are considering the use of Cloud computing or Data-Grids for federating data share common concerns about storage, access, translation and integration. These can be simplified in the following key points

- Where should data be placed and how should it be retained?
- How should data be accessed?
- How should data be presented by one provider so that others will understand it?
- How can one combine data from many distributed and heterogeneous sources?

More specifically the following common capabilities have been identified and developed over OGSA-DAI:

- Data Source Publisher: This capability simplifies the set-up of existing grid middleware by allowing a source of data to be published over web services. It also reduces the ease of use OGSA-DAI, hence lowering the overall entry cost.
- OGSA-DAI Trigger: This capability enhances OGSA-DAI with new data integration features and allows for automated data integration using OGSA-DAI. Underpinning this capability is innovation that allows executing an event-driven OGSA-DAI workflow when a database changes.
- JDBC Driver: This capability offers a new interface for OGSA-DAI that allows enhanced data integration in existing applications and makes integrated data resources appear as a simple database.
- OGSA-DAI SQL views: This capability allows adapting an existing data source for use in a Data-Grid; it enables a view that is independent of the data source and appropriate for use in a Data-Grid without affecting the original data-source.

VII. Common Capabilities for Data and Service Portals

Portals are commonly used as a means of obtaining a unifying view of SOI and Cloud platforms and of introducing transparencies that hide the complexity of the underlying IT infrastructure. They include portals for managing user communities, portals for accessing distributed data sources and portals for managing the life-cycle of computational tasks (i.e. submitting, monitoring in real-time and controlling job). Many businesses considering investing in Grid or Cloud computing have business needs relating to the use of such portals. Based on the analysis of their requirements [5] the strongest business needs for technological innovation in this area were organized in three sub-categories:

1. Security, user provisioning and user management
2. Efficiency and security of file and data sharing

3. Visibility and manageability of submitting, monitoring and controlling transactions, jobs and other computational tasks

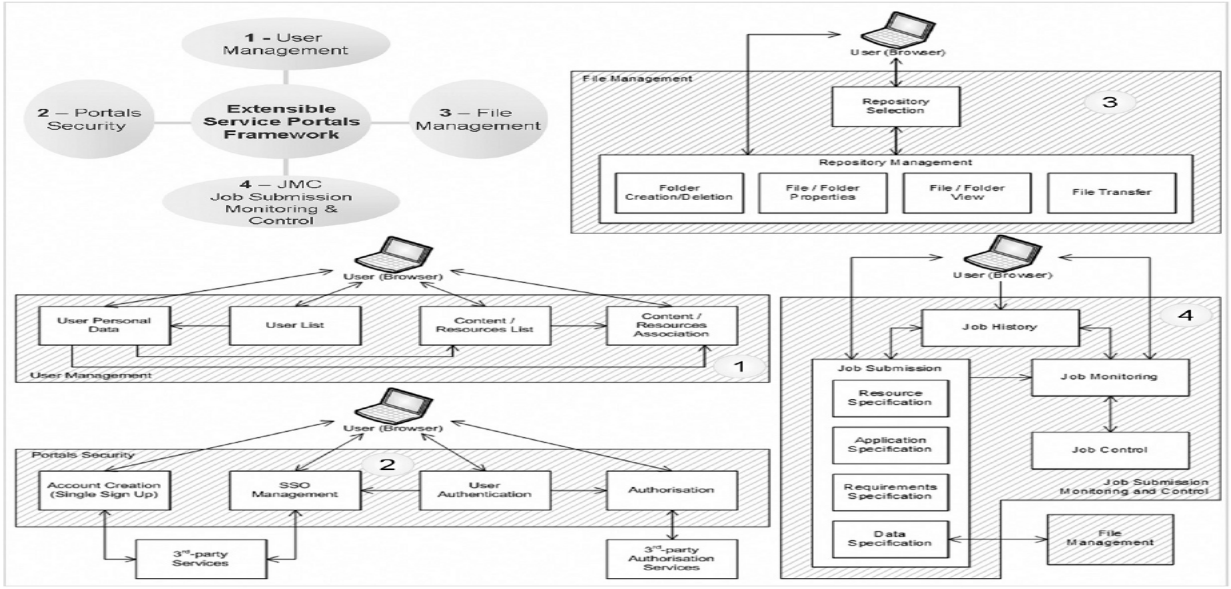

Fig.7 Aspects of an extensible service portals framework for Grid and Cloud computing

VIII. AN EXAMPLE THAT BRINGS IT ALL TOGETHER

The European IT Infrastructure Management Services market was worth almost 50 billion Euros in 2006 according to a report from IDC (IDC 2005) and has been increasing by almost 10% a year until 2009. It appears that a similar trend is now emerging in the Cloud computing area.

According to the analysis at [5] the top four concerns in this area have to do with:

- How to define and enforce security policy
- How to measure and optimize resource usage
- How to monitor and evaluate the quality-of-service offered against an SLA
- How to manage configuration over a federation of hosting platforms

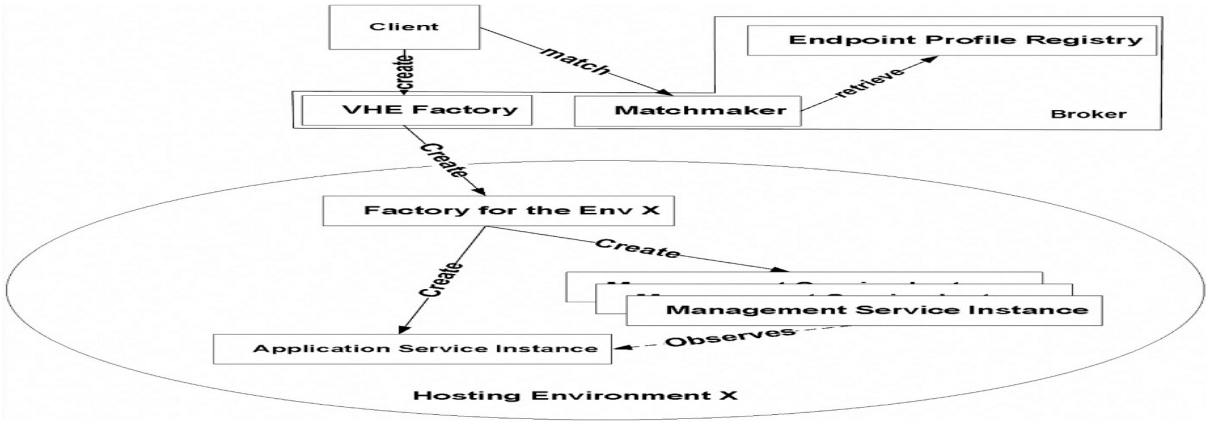

Fig. 8.1 Creation of in-cloud SaaS application instances on an in-cloud Hosting Environment

The ASP is assured by the Broker (representing the Cloud platform federation), based on its visibility of the SLAs provided by the Cloud operators, that the created instance can meet the SLA it has agreed with its customer and is provided with the necessary capabilities for managing the life-cycle of the application instance and the

policies governing the (virtual) service delivery platform through which the application is offered to the ASP's customers. The ASP is not exposed to the complexity and heterogeneity of the capabilities that have been combined in order to allow the application service delivery

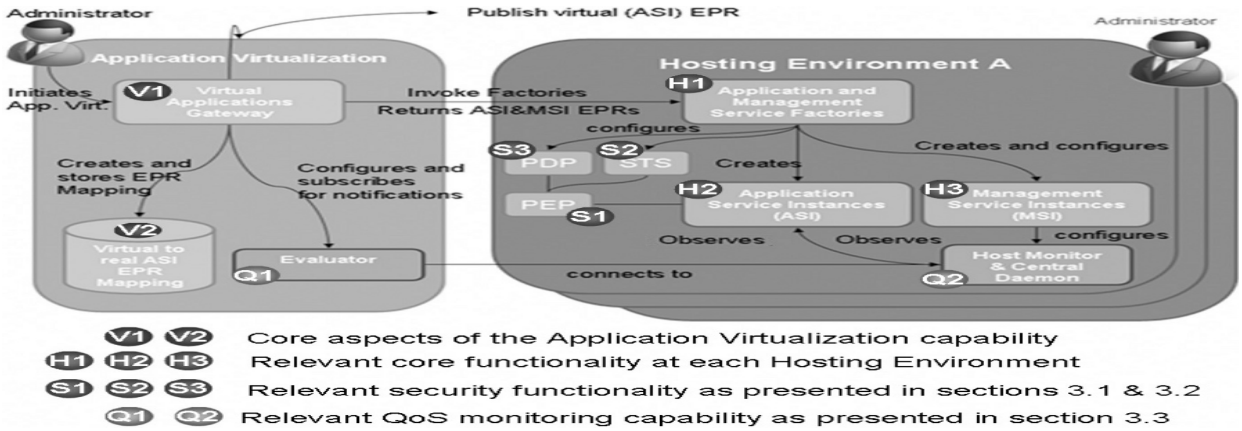

Fig. 8.2 High level architecture of the (enhanced) Application Virtualization Capability

The virtualized application is exposed via an in-cloud service Gateway and the integration of any other value adding services (VAS) – potentially provided by third parties – catering for the non-functional aspects of the application is transparent to the application consumer (see fig. 8.2). The capability enables the ASP to use standardized management services in order to govern the configuration of the virtualized application, the underlying virtual service delivery platform and any third party value adding services (VAS) such as SLA and security capabilities that have been selected by the ASP to enrich the customer experience. The adoption of the Gateway offers the necessary location and platform transparency while acting as an integration point (i.e. a virtual service bus) to external value adding services.

IX. CONCLUSIONS

In our analysis, we highlighted the likely impact of innovation produced by each common capability, and referred to concrete examples of publicly available descriptions of Business Experiments and real-life business scenarios where the current state-of-the-art can be improved by exploiting implementations of these common capabilities. In each case, our analysis included a reflection of the interaction between the technical experts innovating, the business analysts supporting them and a relevant pool of business stakeholders. Such analysis and validation of technological innovation is of an unprecedented size and diversity not only in the history of European research and innovation but also globally.

REFERENCES

[1] www.it-tude.eu
[2] http://www.eu-egee.org
[3] http://www.gridipedia.eu/
[4] http://www.it-tude.com
[5] Dimitrakostheo.dimitrakos@bt.com
[6] Grid and Cloud Computing A Business Perspective on Technology and Applications by Katarina StanoevskaSlabevaThomas Wozniak
[7] Cloud Security and privacy by Tim Mather, Subra kamarasaway , Shahed Latif.