12 Virtual Hosting Environments for Online Gaming

David Bossard, Francesco D'Andria, Theo Dimitrakos, Angelo Gaeta

12.1 General Description

12.1.1 Background

The Virtual Hosting Environment (VHE) is an advanced Information and Communication Technologies (ICT) environment where business services can be integrated with one another across organisational boundaries and domains. The VHE also provides the means to virtualize the environment where the business services operate.

There are two keys areas to be considered as background for this experiment. The proof of concept aimed to provide a novel business service provision solution for online gaming. Online gaming relates to any form of game played over a network with one or more players. It involves in its simplest form a minimum of two computers (that of the player and the game server). In its more advanced form, it uses entire sets of servers, dedicated storage, and playing platforms for massive multiplayer online games (MMOG). The increasing reach of the Internet, the soaring number of connected homes, and the wider choice in technology have contributed to online gaming's rapid growth. The Internet now offers an ever richer palette of games. The gaming industry is thriving: this was true in 2006 at the start of this Business Experiment. According to report by PricewaterhouseCoopers (2009), it is even more true today. Their report estimates that between late 2008 and 2013, the entire gaming market will grow by an average of 7.4 %, jumping from $51.4 billion in 2008 to $73.5 billion in 2013 (PricewaterhouseCoopers 2009). A recent Eurotechnology Japan report states that the Japan Gaming sector alone is booming with the combined net annual income of Japan's top nine game companies overtaking the combined net income of Japan's top 19 electrical giants (Eurotechnology Japan 2009). Online gaming in particular is powering the growth. In the USA, online gaming grew 22% year on year, while console game sales are expected to drop by as much as 20% year on year (comScore 2009). One of the key reasons is the cheapness of online games by comparison to console alternatives. This fuels a greater consumer demand for more readily-available, cheaper, and richer games. In Total Telecom Magazine (2009), Strategy Analytics states "Global revenues from PC and video game software reached more than US$46.5 billion in 2008, of which $6.4 billion or 22% of total revenues was derived from online channels". In addition, "the online share of gaming is expected to continue to rise to an estimated one third of revenues in 2011/12" (Total Telecom Magazine 2009).

However, online gaming is a very demanding market that requires server farms, vast amounts of bandwidth, large storage capacities, rich web gaming portals, and

K. Stanoevska-Slabeva et al. (eds.), *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, DOI 10.1007/978-3-642-05193-7_12,

tools to manage fast-growing user communities. The online gaming industry can expect very fluctuating demands with gaming peaks and lows and irregular usage patterns. To address this, Service Providers (SP) could partner and support game developers to remove the infrastructure burden from them (Total Telecom Magazine 2009) and let them focus on what developers do best – write appealing, highly-interactive, and richly featured games for users to enjoy. SPs would then bring the hosting know-how along with support for a wide array of non-functional requirements such as security and Quality of Service (QoS).

With this in mind, this Business Experiment has analysed the current state of the art (see sect. 12.1.2). It designed a new architecture that supports online gaming providers. It also unlocks internal capabilities at different SP sites to offer them externally as Value-Adding Services (VAS). Such VAS can include billing services, Customer Relationship Management (CRM), or VoIP services (BT 2009b). This has given birth to the Virtual Hosting Environment (VHE) (see sect. 12.2). The VHE is a service-oriented modular architecture able to deliver extensible, flexible, and adaptive scenarios both for online gaming and other service-oriented businesses.

Indeed, online gaming is not the only area that can benefit from the VHE. Any enterprise wishing to embrace the Internet and offer capabilities as a service could benefit from the VHE. Today's organisations are undergoing major changes in the way they conduct business. This requires their IT infrastructure be rethought. Enterprises are increasingly pervasive with a mobile workforce, a rising number of business collaborations with other organisations, and a rising number of externalized infrastructure and services. Many services not seen as core to the business are being outsourced. This is the case for instance of CRM, communications tools (email, VOIP, virtual intranets), and even mission-critical applications such as security. In fact, it is estimated that in the light of today's growing complexity, Small and Medium Enterprises (SMEs) will no longer be able to afford to implement some of the business functions they need and should resort to third-party solutions. In particular, this is the case with security (McAfee 2006). Even worse, many SMEs may not be correctly assessing the risks involved in doing online business while at the same time they "have become very reliant on the Internet" (McAfee 2006). Online access and availability has become very important to the running of businesses.

12.1.2 Limitations of the Current Solution

Current gaming platforms and online gaming providers are built on top of a very static architecture: each online gaming provider buys, runs, and manages its own dedicated game servers. This requires a large initial investment for any new entrant and makes it harder to penetrate the market. It also entails high running costs both from a management and operation aspect as from a maintenance and hardware aspect. In addition, it is extremely difficult to correctly scale the infrastructure as online gaming targets millions of users that will often connect from the same geographical region at roughly the same time for variable periods of time. This generates extreme peaks and lows in demand that impact gaming performance, QoS and ultimately user experience and satisfaction. It shifts the load across the entire

world at different times and would ideally require a geographically-distributed solution.

The online gaming providers' infrastructure is often poorly utilized due to architectural limitations. This can generate ongoing financial losses in addition to the high cost of the initial investment.

Each online gaming provider also needs to implement each core function needed for the running of its business. This includes the hosting and execution of games at the lower end of the overall online game provision; the load balancing between different servers; the monitoring of QoS metrics, service delivery, and customer satisfaction; overall system security and secure messaging; and appealing rich internet applications (RIA) to manage user communities with rich content that drives the overall business. The distributed nature of online gaming, the rising number of users and connections greatly augments the complexity of the systems which in turn will drive online gaming providers to design and adopt easier-to-manage solutions.

On the other hand, service providers currently often only offer communication services, generally limited to the provision of internet and telephony to businesses. However, Total Telecom Magazine (2009) states "service providers could have an opportunity to take some of the infrastructure burden away from games developers and create a new revenue stream. To date network operators have shown more than a tentative interest in online gaming as a new revenue stream. But stellar growth in the gaming market and signs that content companies don't want to manage the whole service end to end, means there could be a greater opportunity for telcos to capitalise on their infrastructure."

The current solution doesn't easily allow for additional VAS to be plugged into it. It is therefore difficult for SPs to provide and bill for such services. The aim of the VHE will therefore be to offer a modular, extensible, pluggable architecture where service providers, businesses, end users, and hosting environments can be brought together to deliver higher-value services.

12.1.3 Requirements for a New Service-Oriented Architecture

In order to address the issues created by static architectures, there is a need to design from scratch a new architecture that can enable the dynamic composition and exposure of Software-as-Services to end customers. Requirements can be grouped into different themes: high-level business requirements, infrastructure requirements, service exposure requirements, governance requirements, and non-functional requirements.

Overall, the key aim of the solution is to develop an architecture that clearly segregates between the actual operations of a business service from the hosting of that service, the network aspects, and the non-functional aspects. The solution should let different providers focus on those areas where they excel.

From a high-level, business perspective, the main requirement is to achieve a new dynamic system that allows cross-enterprise business interactions. This system should be flexible enough so that it can accurately reflect the value chains that exist between the different business partners. The system should offer adequate tools

to offer and measure different levels of QoS based on pre-agreed Service-Level Agreement (SLA) contracts.

The solution put forward should enable each organisation using a Service-Oriented Infrastructure (SOI) to define its own policies to drive their infrastructure. The solution should bring visibility into the execution of these policies. It should also bring visibility and ease-of-management into organisations' relationships with customers, suppliers, and partners.

The solution should be able to leverage existing third-party VAS such as SLA and security services. In particular, it should guarantee QoS to the end customer along with correct billing and QoS measurements. In addition to being able to connect to VAS, the solution should enable organisations to offer their own internal capabilities as VAS: the architecture should enable the secure and controlled exposure of in-house software as services to external customers following the Software-as-a-Service (SaaS) paradigm.

From a core infrastructure perspective, the solution should enable a scalable, extensible, and manageable system capable of reducing IT cost through service reuse and optimization. To achieve this, the architecture should offer a manageable hosting environment where applications can be contextualized, virtualized, and run on the most adequate hosts. It should be possible to combine these environments in clusters or matrixes to provide increased performance. These environments should be highly configurable and manageable to give the end-user (an organisation using these resources) maximized control over its services.

From a security perspective, the solution should support the operation and life-cycle management of trust federations of common capabilities (CC) and business services. By federation, we mean an aggregation of users and services together with an underpinning circle of trust defining the relationship between the different participating partners.

The solution should enable a management and governance model that spans across layers and organisational boundaries in order to achieve a correct picture of the infrastructure, its state, and the services exposed. The governance framework should enable the ability to manage the full policy lifecycle. It should provide the means to audit policies and sub-systems and should be able to prove the compliance of the solution with local regulations, corporate rules, as well as legal constraints both at national and international levels.

Applied to the Online Gaming scenario, these requirements confirm the trend identified in Total Telecom Magazine (2009). Game developers should focus on editing and developing games while buying or renting hosting resources from specialists e.g. Amazon EC2 (http://aws.amazon.com/ec2/). This also confirms the model identified by McAfee. SMEs will either not understand the risks linked with online business models or will not have the means and dedication to invest in an adequately secure infrastructure in order to ensure its business is adequately protected.

The requirements are further detailed in Brossard et al. (2008), Brossard and Prieto Martínez (2009) and Dimitrakos et al. (2009b).

12.1.4 The Business Experiment – Partners and Work Performed

Five key partners took part in the design and development of the VHE for online gaming. These partners are Andago of Spain, ATOS Origin of Spain, BT Group plc of the UK, the Centre of Research in Pure and Applied Mathematics (CRMPA) of Italy, and the University of Rey Juan Carlos (URJC) of Spain.

Andago provided the gaming platform and the business use cases. In particular they fed the initial requirements stemming from the business world and the online gaming sector. Andago also provided (in conjunction with URJC) the resources on which to test the solution developed.

ATOS implemented the service-level agreement (SLA) (monitoring and evaluation) subsystem for the VHE. More information can be found in D'Andria et al. (2008) and in section 12.2.1.4. In particular, ATOS focused on the following issues:

- Automatic resources "negotiation" through an "SLA-based" service advertisement and discovery mechanism.
- Monitoring of agreements, considering network related QoS and the network availability itself as a relevant component of the value chain for service provisioning.
- Platform independent agreement evaluation against the Service Level Objectives (SLO) inside the collaboration contract at run-time.

In addition to leading the overall experiment, BT provided the security services and the technical know-how to integrate them. These services include the federation manager, the identity broker (SOI-STS), the authorization service (SOI-AuthZ-PDP), and the secure messaging gateway (SOI-SMG) detailed in section 12.2.1.3 and in Gaeta et al. (2008), Brossard et al. (2008), and (Brossard and Prieto Martínez 2009). BT also developed the governance gateway (SOI-GGW) which allows the secure management of the infrastructure and full policy lifecycle management.

CRMPA led the integration task of the experiment and also provided the foundation for the hosting environment based on the GrASP middleware (http://www.eu-grasp.net) (Gaeta et al. 2008).

Lastly, URJC integrated the Andago Game Platform (AGP) with GrASP to work in a VHE). URJC focused their efforts on the design and implementation of appropriate integration architecture between both technologies (AGP and GrASP) to provide support for the new business model based on Grid services.

12.1.5 Scenario Description

A network-centric application provider, which in the application example used in this experiment, is an on-line collaborative game platform provider (we shall call it Andago), engages in a contract with the VHE operator (BEMOL) that allows the application provider to use other applications, resources and infrastructure services offered by BEMOL or other parties in order to enhance their user experience. In our example Andago uses game titles from a Game Application Provider; Game Servers offered by other parties (Sunny and Saygah for instance).

Andago can then initiate the creation of a Virtual Organisation (VO) that allows Andago to create instances of a game title from the Game Application Provider on the Game services offered by Sunny Data Centres. Andago use Sunny computational resources in Spain in order to offer collaborative on-line games to Andago's gamer communities. As Andago's customer base expands they decide to expand their VO by amending their contract with the operator (BEMOL) and introducing more game servers this time offered by Saygah. Their decision to expand may be in reaction to surge of use or it may reflect a customer base expansion in the UK, a region for which Saygah Data Centres can offer better QoS than Sunny.

As Andago's customer base expands, they also need to enhance the business intelligence of their network-centric application. Andago may choose to use advanced identity management services offered to the VHE by CHOIR and distributed access management services offered by BEMOL Security. These are network-hosted services that allow Andago to define their own profiles of standards-compliant identity assertions and access control policies. Other business partners of Andago (such as Saygah Data Centres) may choose to use other identity providers (say BEMOL Security) depending on their preferences. The VHE infrastructure ensures compatibility between the different infrastructure services in place. In addition to security services, Andago may want to set-up an SLA framework to measure the QoS that Sunny and Saygah are delivering. It therefore invites ARPEGGIO Quality Services which will deliver a set of SLA monitors and an SLA evaluator to be used as VAS in the VHE.

Different customer relationships over the VHE may be more appropriate for different charging models. For example, Saygah Data Centres and Sunny Data Centres may be charging Andago following a "pay-per-use" model. CHOIR, on the other hand, as an Identity Provider may be charging Andago on the basis of the size or duration of the VO. Finally BEMOL, as a VHE operator, may be charging Andago on a "pay-as-you-grow" fashion based on the portfolio of VHE capabilities that are made available to Andago, while BEMOL may be charging Sunny Data Centres and Saygah Data Centres based on a percentage of their resource utilisation via the VHE and CHOIR a flat fee on the number of customers gained. Such dynamics require very flexible accounting mechanisms offered by the VHE infrastructure in order to allow the various stakeholders to retrieve and correlate chargeable events accurately.

This is a major shift from current state-of-the-art solutions where an online games provider such as Andago would have to invest in hardware and other infrastructure, architect its security and billing solutions, in addition to providing the end-user interfaces, web portals and communities. By delegating hosting issues to specialized providers (Sunny and Saygah), and by delegating security and SLA needs to third-party VAS providers (BEMOL Security, CHOIR, ARPEGGIO Quality Services), Andago can focus on its core business: the provision of an appealing user gaming platform.

12.2 Overview of the Virtual Hosting Environment

The VHE is an advanced Information and Communication Technologies (ICT) environment where business services can be integrated with one another across organisational boundaries and domains. The VHE also provides the means to virtualize the environment where the business services operate. As such, the VHE enables new Software-as-a-Service models that exploit economies of scale for the business service and infrastructure providers; and reduce time-to-market margins by enabling fast service composition and business flexibility.

The virtualisation of hosting environments refers to the federation of a set of distributed hosting environments for execution of an application and the possibility to provide a single access point (e.g. a Gateway) to this set of federated hosting environments.

In the following paragraphs, we will describe the solution developed in this Business Experiment and how it applies to the online gaming scenario.

12.2.1 The Virtual Hosting Environment: Architecture & Implementation

The approach taken in the VHE is that put forward by the Service Oriented Architecture (SOA) paradigm. From an implementation's perspective, this means the experiment has referred to the Web Service Framework roadmap (IBM 2009a) which is currently supported by several commercial SOA platforms and implements service interface specifications and protocols in the WS-* stack that are being standardised mainly in OASIS and W3C.

The core implementation is therefore based on the convergence of Grid and Web Services technology and complies with implementations of the WS-* and WSRF/WSDM protocol stack as well as associated mission-specific standards such as SAML and XACML.

12.2.1.1 Key Concepts

There are four key concepts in the virtual hosting environment (Brossard and Prieto Martínez 2009). These concepts are:

1. The hosting environments
2. The Business-to-Business (B2B) gateways
3. The value-adding infrastructure services (e.g. security and SLA services), and
4. The VO management service

The hosting environment typically represents the physical infrastructure where the applications (for instance the games) are being deployed, instantiated, and executed. It should be possible to manage the hosting environments closely, and monitor the use of resources in order to extract QoS information. Generally, hosting environments can include servers, application gateways, data stores, etc. The instantiation of an application refers to the creation of a unique segregated instance with (possibly) allocated separate resources (CPU, storage) and separate

data stores and state. This instance can then be individually served to customers or organisations.

On the one hand, the B2B gateway acts as an integration point at the edge of the organisation, supporting the virtualisation and secure exposure of application services and enhancing the functionality of these application services, and, on the other hand, by aggregating infrastructure services to implement common non-functional aspects. The latter include QoS obligations, identity federation, access and usage control, etc.

Value-adding services are applications that can be offered as a service over the network and that have as a primary function the support of new application virtualization within different collaborations or contexts. Typically VAS services address critical technical areas that are difficult to achieve for a given organisation for lack of investment, time, know-how, or due to corporate strategies (McAfee 2006). VAS services include identity services, access control services, policy servers, security monitors, SLA evaluators, and so on. In this experiment, the key focus was on security (identity management and bridging, access control, secure policy enforcement) and SLA (SLA monitor, SLA evaluator, SLA-based service selection). Another important VAS is that of the governance gateway which offers the ability to manage business services, infrastructure profiles and full policy lifecycle management during the collaboration lifetime. Other VAS include presence or telephony services e.g. VoIP. An overview of the VAS used in this experiment is given in sections 12.2.1.3 and 12.2.1.4. In addition, we encourage the readers to refer to Gaeta et al. (2008), D'Andria et al. (2008), Brossard et al. (2008) and Dimitrakos et al. (2009a).

The Virtual Organisation Management Service (VOMS) contains a set of services used in the setup of collaborations between different organisations. Typically an organisation will identify a business opportunity and key requirements and technical needs (be it hosting, security, or more complex needs e.g. business processes).

The figure above illustrates the static architectural view of a typical deployment of the entire VHE with several partners as per the scenario elicited in section 12.1.5. Each key component that constitutes the VHE is illustrated: The VOM services are split among partners and the VHE provider. The hosting environments are provided – as per the scenario – by Sunny and Saygah. The game to be run is in Sunny's and Saygah's service pool and will be deployed on their hosting environments. Andago contains its own game web portal which will expose the gaming management interface and user control pane to its end users, the gamers.

In this scenario, the security VAS are provided by CHOIR and BEMOL Security. ARPEGGIO provides the SLA services that will monitor the QoS during the delivery of the services to the end user.

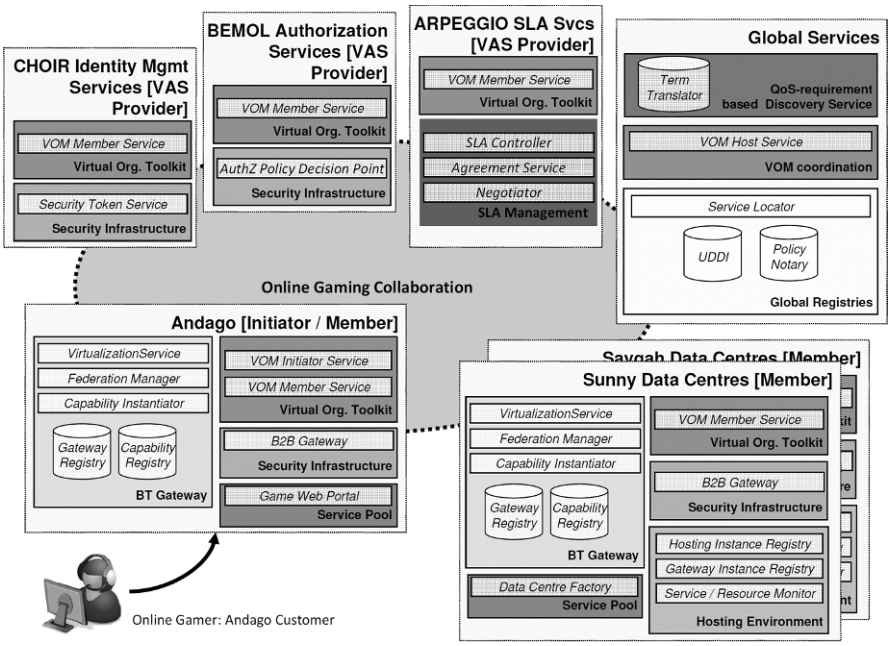

Fig. 12.1: Architectural perspective of the online gaming scenario with the hosting environments, the gateways, the VAS, and the VOMS (Virtual Organisation Toolkit)

The B2B gateways at each participating partner (Andago, Sunny, and Saygah) allow each partner to securely connect to the collaboration and expose their services in a contextualized way. Each participating partner also has a service gateway which handles the instantiation and virtualization of the application instances – in this case the Data Centre factories which will be used to create, host, and run new games instances at either of Sunny or Saygah.

12.2.1.2 Four Steps towards Managed Dynamic Collaborations

Using VOMS, the organisation can follow a rigorous four-step process to create and manage collaborations implemented over the B2B gateway, the VAS infrastructure services, the VOMS, and the hosting environments. These four steps are VO identification, formation, operation, and dissolution. The VOM Coordination Services provided by the VHE operator help liaise between the different partners' VOM member services and manage the lifecycle of the given collaboration (see fig. 12.1).

During the first phase, the organisation identifies relevant partners based on service types they offer and the QoS they guarantee for each service. QoS here relates to high-level customer expectations e.g. a 'gold service experience'. These high-level QoS (HL-QoS) are then translated into lower-level QoS (LL-QoS) such as service latency, CPU usage, and so on depending on the business rules defined. At this time, high-level contracts have been drafted from which lower-level policies and rules can be derived.

In the VO formation phase, the originating partner sends out invitations to the relevant business partners it wishes to invite. An invitation contains the high-level contract or agreement that governs the new collaboration as well as any other low-level policies and rules the originating partner may wish other partners to enforce such as global access control policies. At this point invited partners may accept (or not, as they wish). In a typical online gaming collaboration, the originator may invite hosting environments, game title providers, user base providers, web portals, identity management providers, SLA monitoring providers, and so on. In the online gaming scenario, Andago invites Sunny and Saygah to take part in a gaming collaboration where Sunny and Saygah will be responsible for hosting and executing game instances. Andago also invites ARPEGGIO, BEMOL, and CHOIR to take part in the collaboration as IT solutions providers. BEMOL and CHOIR, for instance, provide security solutions as VAS in the collaboration.

The third phase deals with the operation of the VO. During this phase, new business services previously selected in the VO formation phase can now be instantiated, configured, contextualized, and exposed through the B2B service gateways to the consumers inside the collaboration. The required supporting infrastructure (the VAS) may also be instantiated, configured, and exposed to the collaboration. Instantiation of a business service involves creating an altogether new segregated instance of the service for a particular customer (be it a single user or an organisation), configuring the logical host on which to run the instance (CPU, memory, storage rules and restrictions), configuring the supporting VAS (security, QoS, SLA), exposing the instance to the collaboration, and updating the service instance registries maintained by the VOMS. This step of instantiation, configuration, and contextualization is often called virtualization hence the name Virtual Hosting Environment.

The final phase, VO dissolution, focuses on the removal of the collaboration, the destruction of all created service instances (business and VAS), the removal of configuration files and the reversion to the previous known stable state. In particular, VO dissolution must ensure all systems involved remain in a coherent state and that the registries correctly reflect the business state.

The following figure summarizes the VO lifecycle.

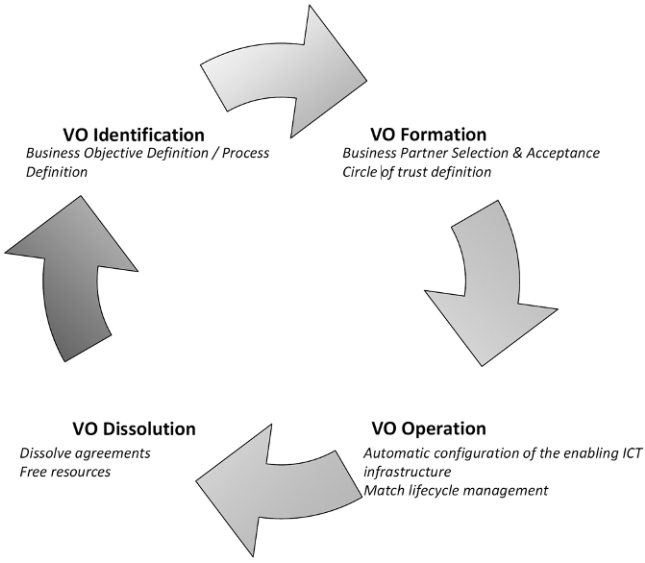

Fig. 12.2: The VO Lifecycle

12.2.1.3 The Security Value-Adding Services

The Security value-adding services used in this experiment were developed by the Trust & Security Theme of the BEinGRID project. This theme includes technical innovation that addresses areas where a perceived and actual lack of security appears to inhabit commercial adoption of SOI technologies. It includes solutions for brokering identities and entitlements across enterprises, managing access to shared resources, analyzing and reacting to security events in a distributed infrastructure, and securing multi-tenancy hosting. These innovations underpin solutions offered in VOM and several other categories.

Out of the work done in this theme, four capabilities have been retained for use in this experiment.

The first capability is a security token service (SOI-STS) which provides Identity and Federation management: it allows, on the one hand, the management of the life-cycle of circles of trust between providers, and therefore the life-cycle management of federation of trust realms, and on the other hand, managing the life-cycle of identities and privileges of users and resources within such federations of trust realms. The obvious benefits of offering these as network-hosted services that can be integrated with application services through the VHE include:

- Facilitating the creation of communities of identity providers that enable identity brokerage and management by supporting open standards such as Liberty Alliance, SAML and WS-Federation, and therefore giving rise to new means of revenue generation. Indeed the SOI-STS can be exposed in the SaaS approach and sold to external customers.

- Enabling the customer to choose the identity provider that is more appropriate for a specific collaboration instead of being locked into what is incorporated in their SOA platform by a middleware vendor or starting expensive product integration projects that give them identity provision and federation, at a very high cost, for the specific application at hand.

The second capability is an Authorization Service (SOI-AuthZ-PDP) which supports distributed access control. It is a policy-based, rule-based access control service which implements XACML, the eXtended Access Control Markup Language (an OASIS standard aimed at defining an access control language to express rich access control rules). It allows the distribution of delegated administrative authority across the value chain. It allows managing the distribution of administrative authority among multiple partners (e.g. providers of applications, of application hosting, of identity services, etc.) and the management of constraints about the scope within which each administrative authority can operate.

The delegated access control mechanism explored in this experiment allows finely granular control on the delegation of administrative authority. In particular, management and access policy can be signed on behalf of different administrators and evaluated at run time against delegation constraints that discount parts of the polices and resolve conflicts in accordance with the identity and role of each administrator. This allows for example the VHE operator to profile or constrain the policies that an Application Service Provider (ASP) administrator can define, and their period of validity. The ASP administrator can then define whatever access policies fit their application best, including policies that allow a collaboration manager to fine tune the certain aspects of the access for a limited period of time. For example, the VHE operator may have constrained that the ASP cannot deny access to information about the services it provides to another legitimate customer of the VHE. The VHE operation may have also constrained that an ASP can only define policies about services offered in those collaborations they can join according to their subscription to the VHE. Then the ASP will have full control of access to the applications they offer in collaborations that they are allowed to join but will not be able to hide information about the service they offer within the VHE. In addition to access policies about the services they offer in those collaborations, they may also define a constraint that allows the collaboration manager to fine tune access to resources during a promotion period. Therefore the collaboration manager could override a policy denying game service access to "bronze" members to a "limited-edition" game but only during the promotion period.

This capability offers an essential service managing distribution of the administration tasks across the value chain while assuring accountability and non-repudiation of administrative actions during the operation of a distributed infrastructure.

Thirdly, the secure messaging gateway (SOI-SMG) is a network- or perimeter-hosted policy enforcement point that can be itself configured through an extensible policy language. It brings together selected functionalities from XML firewalls, application gateways, content inspection and transformation engines, light-weight enterprise service / event bus, and network resource management. It can securely

expose services on the basis of network traffic, message content, and application data. It acts as a message interceptor, decorator, router and enforcer. It is also the integration node in an SOA deployment (as in this scenario). The SOI-SMG being policy-based allows for rich, highly adaptive scenarios. The SOI-SMG can be used in several collaborations concurrently while maintaining clear message flow segregation.

Lastly, the governance gateway (SOI-GGW) focuses on the management and governance of infrastructure and capability profiles. In particular, it provides the ability to define security infrastructure profiles that associate the business service to be exposed with a unique combination of virtual service endpoint and collaboration context, and with

- A collection of one or more application gateways (SOI-SMG),
- A collection of zero or more VAS (SOI-STS, SOI-AuthZ-PDP…),
- A collection of security policy templates to apply for each VAS
- A configuration management process reflecting a common policy management life-cycle

It also provides a process to manage the life-cycle of the business service being exposed in accordance with a selected profile. This process includes sub-processes for exposing the service in the given context, binding the corresponding value-adding security services and managing the applicable policy instances for each of these value-adding security services.

These capabilities integrate as illustrated in the figure below. The integrated view illustrates part of the operational phase of the gaming scenario.

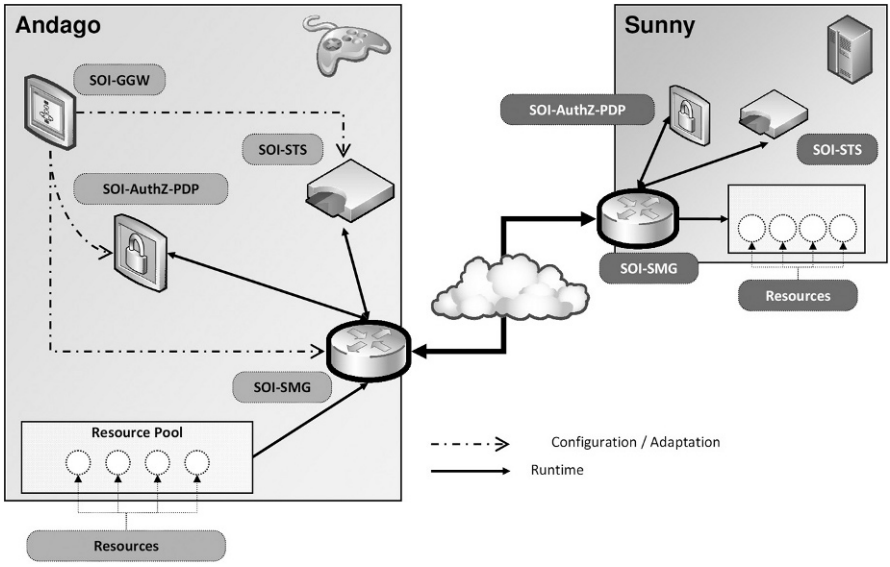

Fig. 12.3: An integrated view of the Security VAS

Figure 12.3 proposes a zoom on the security infrastructure being used in the proposed architecture as illustrated in figure 12.2. This figure abstracts away the organisations which offer the services. Figure 12.3 clearly shows that the SOI-SMG is the underlying VAS to the B2B security gateway mentioned in section 12.2.1.1. Once correctly configured on a per-service, per-context basis, it integrates several value-adding security services namely the identity broker (SOI-STS) and the authorization service (SOI-AuthZ-PDP) to protect service invocations from Andago's services to Sunny's services where the game instances are being executed. In particular the SOI-SMG at Andago will check that the initial request comes from a valid user who is authorized to proceed with such a request. This involves checking for the identity of the requestor, checking whether they are a member of the current collaboration, and checking whether there is an existing identity mapping definition for that particular identity. If so, Andago's SOI-STS delivers a virtual identity token which is then used for authentication by Sunny where the token is validated and checked for identity claims that describe the initial requestor and which can be used for access control decisions at Sunny's SOI-AuthZ-PDP. Details of this interaction are further explained in section 12.2.2 as well as in Brossard et al. (2008) and Dimitrakos et al. (2009b). This service-oriented model brings context-aware, content-aware security to the application layer and as such brings flexibility and enables dynamic service composition models.

12.2.1.4 The SLA Value-Adding Services

The SLA value-adding services consider two well differentiated phases: firstly, the advertisement and discovery of the Business Service / SLA Contract and, secondly, the monitoring and evaluation of its fulfilment at run-time. In the experiment the L&D subsystem extends the classical Universal Description, Discovery and Integration (UDDI) directory functionalities in two areas:

- It allows the publication of business services against the directory through an automatic mechanism.
- It allows the classification of business on the basis of metadata that describes QoS information contained in the associated SLA pre-contract.

In the gaming scenario, when a Game Provider deploys a new game, he also publishes an SLA Template (or SLA pre-contract) associated to that game with specific QoS that should be guaranteed. These QoS parameters cover infrastructure, performance and network parameters, such as CPU use, latency or memory, which will be called low level (LL) parameters. The game provider then defines an XML-based mapping policy which maps the LL-QoS into high level (HL), human understandable, QoS parameters.

At search time when the on-line game (OLG) clients (Gamers) want to look for a service (game), the "human understandable" HL QoS parameters are specified as search criteria: e.g. Graphic Resolution or Available Resources. Using the mapping capability provided by the VHE the L&D, the Service Directory is queried for potential Service Providers that are able to offer the most suitable service to

the client as shown in the following figure. Finally the business service (in this scenario, a match for a given game) and its associated SLA Contract are delivered to the Gamer.

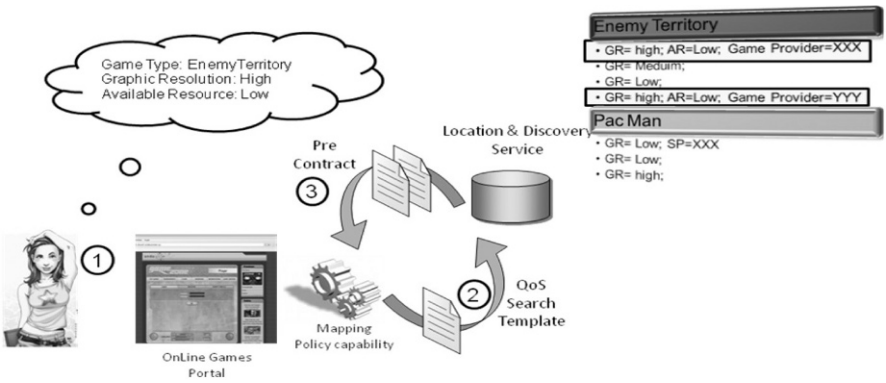

Fig. 12.4: High-level to Low-level QoS requirements mapping

After the business service has been delivered, it is necessary to ensure that the contractual terms are respected. This is done though the Monitoring and Evaluation subsystem (M&E). The M&E subsystem is logically divided into three main blocks:

- Application-specific monitoring: offers the ability to retrieve at run-time information about the users participating in a game, and other general information about the match like its lifecycle, number of users playing the match and some game statistics;
- Infrastructure monitoring: offers the ability to monitor resources virtualized as Grid services. In this experiment, it is possible to monitor parameters like the CPU cycle and the memory consumed by the match (service instance) at runtime;
- Evaluation layer: offers the ability to collect (through the two above mentioned modules) the monitored values in order to verify whether the measurements are within the thresholds defined in the SLA contract assigned to every player. Whenever the execution of a match does not satisfy these SLA conditions, the module will launch a notification event (using a WS-Notification mechanism) about this potential breach of contract.
  More information can be found in D'Andria et al. (2008).

12.2.2 Online Gaming Scenario at Runtime

The gaming scenario is perhaps best told from the end user's perspective. In online gaming, a user typically wants to play a game online within a community of liked-minded players. He wants to take part in various games where other players play as well as he or she does. Response time and availability are therefore critical. So is the overall security of the underlying systems. The player's interaction starts when

he goes to the Andago website to play a game. Provided he has a valid account, he can log into Andago's web portal which manages users, games, and online communities. On the richly-enabled website, the user can choose a game he wishes to play. Andago decides to advertise certain game titles depending on agreements with game title publishers. Up to this point, all interactions take part solely between Andago and the end user and therefore neither the VHE nor its enabling B2B gateways are in play. However the richness of Andago's offering is a direct consequence of its ability to form dynamic collaborations with different provider. Once the player has selected a game, e.g. EnemyTerritory, he can choose a match to take part in. This is where the VHE and the B2B gateways kick in. A match is in fact a given specific VO with a virtualized exposed application instance for one of the game servers (GS) selected e.g. either Sunny or Saygah.

Once the player has selected a match, Andago will kick-start the virtualization of its own client application which liaises between the Andago platform and the hosting environment's virtualized service. In this scenario, Andago exposes a management client called Agasy. Therefore at this stage Andago is virtualising and exposing a contextualized instance of the Agasy at its B2B gateway. The Agasy instance will be exchanging management and monitoring messages with the virtualized game watcher instance at either Sunny or Saygah. This watcher continuously monitors the state of the running game instance on the host server and sends back gaming operation statistics to the Agasy instance. Every time the client instance running behind Andago's B2B gateway makes a call to the virtualized watcher instance at either Sunny or Saygah, the request goes:

- through Andago's gateway where
  - it is checked and decorated with the appropriate virtual identity (e.g., a SAML token) issued by the SOI-STS for the given instance
  - checked against client-side authorization rules
  - encrypted for transport between the partners' gateways
  - sent to the partner's gateway, i.e. Sunny or Saygah
- through the receiving partner's gateway where
  - the SAML token is extracted and sent to the STS for validation
  - the STS validates the virtual identity (SAML token) and returns the associated identity attributes for the given requestor
  - the gateway decrypts the message
  - the gateway requests an authorization decision from the SOI-AuthZ-PDP based on the XACML attributes extracted from the SAML token and based on the originating client and targeted service
  - the gateway forwards the request to the internal service i.e. the watcher

During the execution of the sequence of these interactions, the relevant infrastructure services, in particular the SOI-SMG and the application instances, feed events into the SLA monitoring services in order to evaluate the status of the infrastructure and to determine whether any service provider is breaching the agreed contract.

Thanks to the B2B gateway, the message exchange is secured and therefore allows Andago to monitor the hosting environments. It can determine how much to pay Saygah and Sunny depending on the usage as well as on the experience delivered (reliable hosting or not for instance).

12.3 Business Benefits

12.3.1 Customer Benefits in Online Gaming

There are different customer types that can benefit from the VHE approach. Firstly, the end user or gamer will indirectly benefit from the VHE as he will be given a wider range of games at different levels of quality with more adequate and competitive pricing models.

Secondly, traditional service providers (SP) who contented themselves with providing raw communications services (typical of ISPs) will now be able to offer additional capabilities as services in a SaaS approach. Such services include, as already mentioned, identity and access control management services, encryption services, SLA services, CRM services, telecommunications services (call-backs, the sending of SMS, etc), and generally any capability the enterprise has internally and is willing to share with external customers in order to generate revenue. This has been clearly identified in Total Telecom Magazine (2009). In particular it highlights that the "huge cost of developing massive multiplayer online games (MMOG) could mean an increasing opportunity for network infrastructure and data warehousing service providers as games publishers increasingly try to move away from providing the end-to-end 'vertical".

Thirdly, game developers and web gaming platforms also benefit from the VHE approach as they can focus on developing new game titles and creating appealing user platforms without having to worry about the details of operating the platform, the game, or any of the underlying infrastructure along with the non-functional requirements (such as security and QoS) these bring. Again, Total Telecom Magazine states that "because MMOGs are persistent online games that are commonly played by hundreds or thousands of players on one hardware server at the same time, support costs can be high". These costs need to be controlled and driven down. Piers Harding-Rolls (a senior analyst at Screen Digest) states that "a popular game might have tens of servers each with a few thousand players". This is the main cause for the expensive infrastructure and maintenance when owned and operated by the game developer. A pay-as-you-grow or pay-as-you-go provision model can help reduce such costs.

12.3.2 The VHE as an Enabler of the SOA Approach

The VHE enables the customer to adopt a low risk approach to SOA deployment and increases Return on Investment (RoI). The VHE provides common, shared technologies that enable business processes to be added and changed easily. Expensive infrastructure is pooled, decreasing the support and maintenance costs, allowing

for a greatly reduced capital outlay, and increasing utilisation of the IT resource. Implementing a service-oriented design facilitates increased collaboration with both customers and suppliers, and offers opportunities for a higher degree of service composition and process automation across the value chain. The VHE also offers common capabilities meeting non-functional requirements such as:

- Business collaboration management,
- Service publication, service categorization and discovery based on high-level QoS requirements,
- Process driven service composition,
- Federated identity and access management,
- SLA monitoring and evaluation, and
- Secure messaging and content validation, content-based routing.

This experiment validates the use of VHE as an enabler of collaborative online gaming services. Validation is achieved by implementing a gaming platform (provided by Andago) on the top of a VHE specialisation for on-line collaborative gaming. The VHE helps businesses to improve their "concept-to-market" development cycle. This is achieved by leveraging the common capability integration and process-driven service and resource composition that is enabled by the VHE infrastructure. The VHE should enable a 25% – 50% reduction of the concept-to-market cycle, especially in cases where services are composed for the first time in response to a new market need (Sawnhey 2005). The VHE should also help businesses optimise their "right first time" ratio by leveraging the flexibility offered by policy-based management of the VHE infrastructure and its ability for autonomic adaptation in response to contextual changes. The VHE should allow an 80% or higher "right first time" ratio for exposing composite services on the VHE, especially in cases where reconfiguration is required in order to respond to changes of service usage or access requirements (Sawnhey 2005). The VHE proposition offers the potential to treat both IT and business functions as a series of interconnected services—from activities like HR and travel that serve employees, to sales, to managing customer identity and access, to delivery and other activities that serve customers. It offers organisations new ways to selectively outsource, to quickly configure and reconfigure these services to continually maximize efficiency, even as their business world changes.

From a customer's perspective SOI provides a very compelling story, incorporating the attractive aspects of SOA with flexible, cost effective infrastructure. Current estimates (IDC 2006) are that between 50 – 80% of enterprises are planning and deploying SOA to achieve the following:

- S*ervice reuse*: accelerated implementation of new business functions and changes to existing ones, lower effort and risk, reduced cost, quicker implementation;
- C*omposite applications built by combining services*: *Rapid response* to changing market requirements and *first-to-market* competitive advantage. *Optimization of end-to-end processes* rather than just individual activities

- L*oosely coupled systems*: greater flexibility, increased implementation agility, improved process efficiency, and a higher degree of automation.
- S*tandards-based end-to-end security*: greater interoperability; controlled exposure of business functions to business partners; managing (and hiding) infrastructure complexity; guaranteed compliance with higher-level enterprise policies including the implementation of *regulatory requirements* and ability to *prove compliance* with these.

VHE customers can select productised components from a menu of options, each with its own service level (speed, capacity and/or availability) and pricing model. Under the VHE, customers' demands are becoming more service-based and Service Level Agreements and Guarantees (SLAs & SLGs), as well as Identity, Security and Access policies, are more focused on business requirements. Instead of defining network or application availability related guarantees, customers will require a range of service level performance options based upon end user requirements and business metrics.

12.3.3 Business Benefits in Other Market Sectors

Essentially, the VHE product is a network-centric Service Oriented Infrastructure to be used by enterprise networks. Enterprise network scenarios range from defence coalitions, to multi-site finance institutions, multi-party logistics support, and aggregation of entertainment and media services. The VHE allows enterprises to expose interfaces to internally-hosted services in such a way that they can be combined easily and securely with services contributed by other business partners on demand. The three main markets in priority are:

- Defence coalitions (e.g. coalitions between NATO members)
- Multi-provider VAS integration for entertainment and gaming (such as BT and Sony's Go! Messenger offering (BT 2009a))
- Large-scale corporations with a multi-site IT infrastructure including those arising from a series of mergers and acquisitions

One motive for emphasising large corporations and coalitions as early adopters stems from the up-take of an SOA strategy in such organisations and the willingness of some of these customers to make a substantial investment on innovation in order to solve challenges in the Managed (IT) Infrastructure Services area. Once an operational infrastructure is established, we expect it will also be particularly valuable for smaller companies who want to earn money out of innovative web services. In the future, we envisage the enterprise networks using the VHE platform being clusters of SMEs within a given market sector. However, in the short term, the VHE offering is being driven by the needs and investment of large corporate customers and government departments (especially defence).

12.4 Lessons Learnt

Over the course of the two years during which the Business Experiment ran, several lessons have been learnt as to the choice and development of the technology, the chosen approaches, the architecture put forward. Additional lessons relate to the customer's expectations and its management.

12.4.1 Organisations' Main Motivation to Migrate to SOA

In his SOA Maturity Model, Theo Beack, Chief SOA Architect at SoftwareAG, summarizes the main issues faced when interfacing with new customers: "Organisations are all inundated with information about SOA and the steps [this] require[s]…" (Beack 2006). The first lesson to retain is that SOA confuses many decision makers when wondering whether to make a strategic move which may halt or hinder an enterprise's IT operations over a significant period of time during which the transition takes place.

To avoid this adverse reaction, the customer, be it the online gaming platform provider or any IT enterprise, needs to have the key benefits delivered by the VHE clearly explained. The latter brings a clear roadmap to SOA adoption along with the adequate tools and an architecture that allows growth and expansion. It is important to accompany enterprises in their migration by supporting them with a clear plan. The VHE should first provide a point of reference which is the main aim of the SOA realization. Based on that reference, the organisation should create a common vision and understanding of what it wants to realize with SOA and what it means for its IT operations and business in general. In a later stage, the organisation should identify gaps between its current state of the art and what it wants to achieve. Lastly, before deciding to proceed, it should prioritize and measure the impact of SOA and the VHE on its business and in particular try to measure the Return on Investment (RoI) to determine whether it is worthwhile. An additional stage in this plan should consider, prioritize and plan actions for improvement of the architecture being put forward. Only with the adequate framework will enterprises become less reluctant and start adopting the VHE.

Another key aspect that is increasingly proving useful to incite enterprises to adopt an SOA strategy is the ability to cut operation costs (mainly electricity used in running servers and the necessary cooling equipment) and the linked environmental concern. A recent article in the Wall Street & Technology Journal (2009) highlights that more and more Wall St. firms are turning to SOA architectures and virtualization technologies to cut their electric bill and become greener. This approach is helping them to save their energy consumption and generally helps them reduce manpower and "do more with less". This is in line with current IT budgets which are suffering massive cuts due to the 2009 recession. Where enterprises were once reluctant to evolve to an SOA or VHE approach, the current financial situation is forcing them to.

Enterprises can also particularly benefit from this approach by generating profits from once locked-in value-adding services. BT, for instance, has launched in March

2009 a virtualised infrastructure service which involves the virtualisation of servers, storage, networks and security delivered to customers via an online portal as Cloud-based services (ZDNet UK 2009). By doing so, BT is in fact offering capabilities it already provides internally for its own operations and is optimizing resource usages and selling them to generate additional revenue. Other common capabilities included in the telecommunications sector are Voice over IP (VoIP) services, call-backs and call flows, text message services such as the ones offered by Ribbit (http://www.ribbit.com/). Going to other organisation with success stories – such as BT's – will help them in their own adoption of the VHE and the SOA paradigm in general.

12.4.2 Risks Associated to SOA

Changing to an open, service-oriented model comes with technical pitfalls addressed in the VHE but that should not be overlooked by organisations. In particular, a distributed system with multiple components that potentially span across different organisational domains needs adequate management tools: governance is therefore critical to control this complexity. This governance process should be based on a well-defined set of interface guidelines and policies.

Secondly, the governance process should provide the means to manage those policies that matter and provide tools to manage the entire lifecycle of the policies from its initial template stages to their execution. Policies should have issuers. The latter should not be able to repudiate the policies in order to ensure compliance with regulations and laws both inside the enterprise, within the dynamic collaboration, and within national and international legal frameworks.

Thirdly accurate governance should come with the identification of asset owners, administrators and generally speaking those responsible for maintaining the services with which an enterprise is to integrate.

Lastly, from a more technical perspective, if SOA is to be fully achieved, particular care is to be put on the definition of service interfaces and contracts. In particular, those interfaces should enable loose coupling.

12.5 Conclusion

In the past, many companies' strategic business planning relied upon forecasts of future market conditions and customer needs over time periods of one to five years. In the stable business environment that then existed, companies could take their time to plan and develop a suitable IT infrastructure because market conditions and customer needs were relatively stable. But in today's uncertain business conditions, it is difficult for companies to look that far into the future, with any certainty. Instead they have to spot trends early and respond more quickly than competitors to new opportunities and threats. However, many enterprises are finding that their ability to innovate and execute new business strategies is being constrained by the inability of their IT infrastructure to support these new strategic initiatives. If so, these customers need to transform their existing inflexible IT infrastructures into

more flexible and agile infrastructures that can support new and innovative business strategies in shorter time scales.

In response to such customer needs and insights, this experiment has developed the VHE proposition. The VHE offers the potential to treat both IT and business functions as a series of interconnected services. It is an attempt to offer organisations new ways to selectively outsource, to quickly configure and reconfigure these services and to continually maximize efficiency, even as their business world changes. VHE is an enhanced Service Oriented Infrastructure (SOI) that is built on the fusion of:

- The SOA for ensuring composition of loosely coupled services
- The virtualisation and distributed management of ICT resources based on Grid computing
- The management of Network resources based on a federated architecture.

The pull for the VHE has mainly come from two areas: the need for enterprises to become more flexible in order to adapt to evolving business models leading to new revenue-generating opportunities and the increasing pressure to reduce operating costs.

Other reasons come from the need to reduce organisations' environmental impact by reducing energy consumption as stated in Wall Street & Technology (2009).

Between the completion of this experiment in June of 2008 and now, the Grid SOA paradigm has evolved into the Cloud computing proposition. Many leading IT organisations including telecommunications providers such as BT and Orange are investing in Cloud computing proposals. Indeed, Gartner predict 22% growth in 2009, with revenues reaching $9.6bn and rising to $16bn by 2013 in the Cloud computing market (MicroScope 2009). A trend toward Cloud computing is to be expected in the light of the challenges faced by major Wall St firms. The VHE approach taken in this experiment has been built in such a flexible way that it can be easily migrated towards a Cloud approach with little or no effort.

Cloud computing will also impact security services because we expect to see a new Security-as-a-Service model emerge. With technology dissolving traditional network boundaries and companies changing their operational business models, Cloud-based security will be essential. The work in identity and access management done in BEinGRID and this experiment fit naturally into the Cloud.

The results of this experiment are extremely encouraging. There is a very dynamic market with very high expectations for new SOA-oriented visions in order to pursue new business opportunities, cut IT operation costs, and fuel the corporate green agenda which is becoming important in Corporate Social Responsibility (CSR) strategies. We believe large IT corporations (consultancy firms, telecommunications providers) should lead the way into the Cloud computing paradigm. The partners of this experiment and in particular ATOS and BT can leverage the results of this experiment to strengthen their respective proposals.