A Service Oriented Architecture to support the federation lifecycle management in a secure B2B environment

Angelo GAETA[1], Francesco ORCIUOLI[2], Nicola CAPUANO[2], David BROSSARD[3], Theo DIMITRAKOS[3]

[1]*CRMPA, via ponte don Melillo, Fisciano, 84084, Fisciano (SA)*
Tel: +39 089 96 43 64, Email: agaeta@crmpa.unisa.it
[2]*DIIMA, via ponte don Melillo, Fisciano, 84084, Fisciano (SA)*
Email orciuoli@diima.unisa.it, ncapuano@unisa.it
[3]*British Telecommunications plc, Adastral Park, Martlesham Heath, IP5 3RE, United Kingdom*
Tel: +44 1473 606149, Email: david.brossard@bt.com, theo.dimitrakos@bt.com

Abstract: This paper presents a Service Oriented Architecture to manage the lifecycle of a federation in a secure Business to Business (B2B) environment. The main contribution of the authors to Grid and SOA communities is related to the definition and development of a set of design patterns and software components to support the creation, management and dissolution of a federation of different administrative domains. As case of study we present the application of our components to a concrete business scenario relating to the on-line game application provision, providing also an overview of the main business benefits assessed during the evaluation of the components.

1 Introduction

The paper has the objective of presenting design patterns and software components, based on Grid and Service Oriented Architecture (SOA) technologies, to address the issues related to the federation lifecycle management in a secure B2B environment. In contrast to the current state of the art, that is mainly based of results coming from the eScience community, such as VOMS [4] or GridShib [5], the solutions proposed take into account the needs and requirements of the business communities. This aspect has had a deep impact in the design and implementation of the proposed software components.

While, in fact, most of the eScience solutions propose and implement coarse-grained models to address issues related to membership and management of resources in a Virtual Organization [1] (for instance, allowing the access to a whole resources for job submission) in our case we have requirements that foresees a fine-grained approach (for instance, allowing the access to specific capabilities offered by a Service Provider).

The results presented in this paper are part of the EU FP6 Business Experiments in GRID (BEinGRID) project [6] that is focused around two complementary activities. Firstly, the project is undertaking a series of Business Experiment (BE) pilots designed to implement and deploy Grid solutions in a broad spectrum of business sectors. Secondly, a toolset repository of software components is created to support European businesses that wish to take-up this technology. The work to produce the contents of the repository is divided up into a number of technical Clusters. In BEinGRID project, a Cluster is a thematic activity that focuses on particular technical area relevant for Grid, and produces

patterns and generic components by analysing independent requirements and designs provided by each one of the sector-focused pilot projects.

The Clusters defined in the project are: Security, Virtual Organization Management, Service Management (including Service Level Agreements), Data Management and Portals. This paper is concerned with results of the Security and Virtual Organization Management Clusters. For the purpose of this paper, we focus our attention on the issues relating to federation lifecycle management in a secure B2B environment.

The rest of the paper is as follow. In section 2, we briefly recall the methodology adopted to elicit requirements in order to define the patterns and software components, in section 3 we present the software components, and in section 4 we present the case of study. In sections 5 and 6 we discuss main results and business benefits and, eventually, in section 7 we draw our conclusions.

2 Methodology

The methodology followed to define the components is based on the analysis the BEs. We extract requirements from BEs, identify architectural capabilities and produce design patterns and components. The approach, therefore, is driven from the concrete necessity of the BEs rather than from the theoretical benefits of the Grid technologies.

The BEs selected for analysis cover several vertical markets, including the following: Civil Architecture (BE03 [11]), Retail (BE05 [12]), Leisure & Entertainment (BE09 [13]), Chemistry (BE14 [14]), Finance (BE15 [15]). This diversity further strengthens the value of the results and the commonality of the requirements identified.

It became apparent during the analysis that the business communities are currently more interested in simplifying the management of heterogeneous resources in *a federated business environment* than the dynamicity of the life-cycle of Virtual Organizations. In particular, the BEs analysed present common requirements mainly related to *accessing and managing in a simple and secure way* heterogeneous distributed resources shared among the organisations participating in a collaboration, and issues relating to resource discovery and application/service deployment.

Another key problem that emerges from this analysis is the *dematerialisation* of the ICT infrastructure underpinning Virtual Organisations: application and ICT resource providers want to reduce or outsource the overhead, also in terms of cost, of managing the distributed Service-Oriented Infrastructure that underpins their Business-to-Business collaborations.

3 The software components

As evidenced in the previous section, common requirements derived from the analysis of the BEs relate to a trend towards either outsourcing or reducing the costs and overhead of managing a shared distributed infrastructure, to simplify access to (and management of) the infrastructure's resources, to support the deployment and distribution of applications on the infrastructure without compromising security or quality-of-service.

This indicates the need for common capabilities and patterns that allow ASPs, ISVs and other providers of business applications to concentrate on the application management and the application service exposure / provisioning to their customers without having to deal with the infrastructure management or administration

In the following subsections we present the main components developed to address the requirements and common capabilities resulted from the BEs analysis. Details on the associated design patterns are presented in [3] and in [7].

3.1 VO set-up

This component is required to set up relevant information of a B2B collaboration.

During the VO identification & formation phases, in general, there is the need to perform operations like configuration of the infrastructure, instantiation and orchestration of the application service, assignment and set up of resources and activation of services, notification of the involved members, and manifestation of the new VO.

The high level architecture of this component is presented below:

- *VO Set-up*: this is mainly a façade interacting with the other components.
- *Registries*: these contain new members and service instances of the VO.
- *Federation*: this is in charge to create a federation and to manage the identity of the federation members. This component can be designed according to the Secure Federation Design Patterns [8] and other patterns proposed by the security area of the BEinGRID project such as the Security Token Service one [9] – see below for further details on the STS.

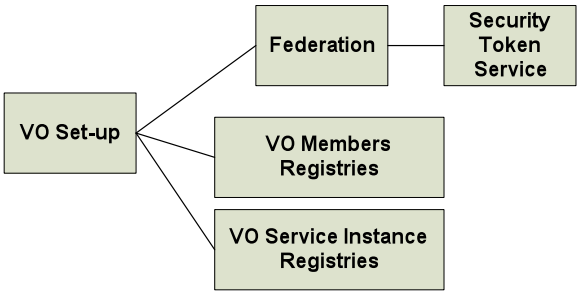

Figure 1: VO Set-up

The component is useful in several concrete scenarios where there is a low level of dynamicity in the VO (meaning that the other steps of the creation process, such as agreement negotiations and policy definition, may be performed off-line). The federation manager of this component implements and extends the TrustCoM model [16] and is detailed in the next section.

3.2 *B2B Federation Management services (FMS) and Security Token Services (STS)*

The STS acts as an identity broker for each enterprise, and manages the correlation of identities and security attributes within a security domain with commonly understood credentials across domains. It allows:

1) managing a local participant's perspective of a circle of trust, and
2) adapting local authentication mechanism, token scheme, identity token transformation scheme based on contextual information, secure remote management.

The STS pattern originates research by BT and Microsoft (EMIC) in the TrustCoM project [18].

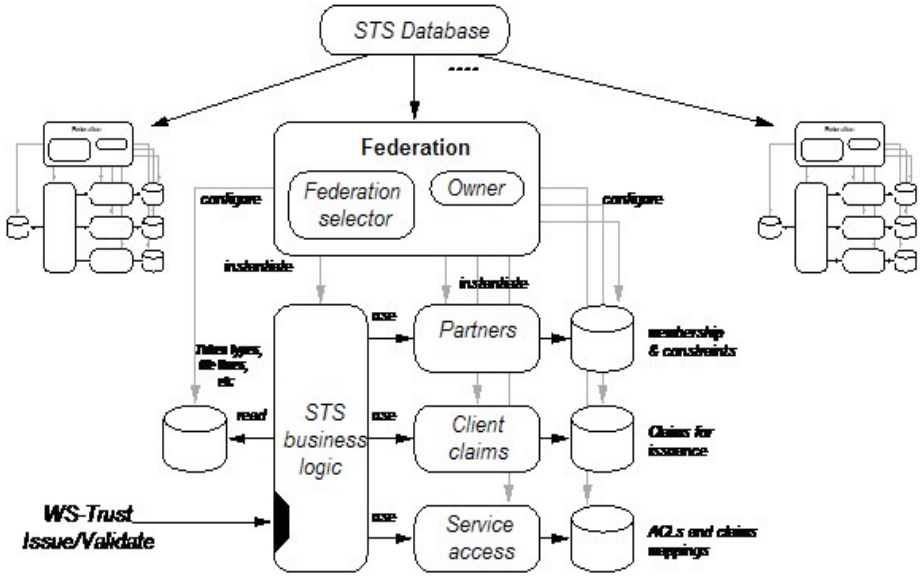

Figure 2 - Federation and STS

The key features of this design include:

Context-driven adaptation: A "context selector" inspects issuance, exchange or validation requests for a context element – typically a WS-Federation identifier - and depending on this selects a configuration from a repository including:

- a business logic explaining how to do the issuance or validation
- a set of security modules implementing info-sets & actions, such as: token format, internal identity profile, inter-organisational claims profile, token signature scheme.

Consequently the observable STS behaviour is different for different federation contexts, and adaptation to a federation context happens at real-time depending on the context of the request.

Contextualisation of token issuance: The same internal resource X – identified by its internal certificate - can be issued different token in content depending on the context of the request. The context of the issuance request is configurable: e.g. Federation identifier, resource to contact, action to be performed, etc. The functionality for issuing or exchanging security tokens (including the token format) is extensible, supporting, for example, custom XML tokens, SAML assertions, and X.509 certificates at the same time.

Manage circle of trust: Each STS holds signed statements identifying the other STSs in a circle of trust and an explicitly defined federation identifier. It also accepts a "local federation context owner" and allows the creation of an association of a global federation identifier with the group of participating STS identities and the identity of the local owner of the federation. The local owner (administrator) manages the local view of the circle of trust underpinning the federation.

The Federation Management Service (FMS) allows managing the full life-cycle of circles of trust, by coordinating a distributed process that establishes trust between the participating STSs. The model allows for STS allows creating asymmetric views of a circle of trust. For example:

- A, B, C participate in the same circle of trust FedID
- A recognizes token issuance authority of A, B and C in FedID
- B recognizes token issuance authority of B and C in FedID
- C recognizes token issuance authority of A and C in FedID

3.3 Policy Enforcement Point

The PEP is an adaptable policy enforcement component that does SOAP level processing on behalf of an application service. In addition, by exposing the application at a given endpoint on the PEP itself, it effectively virtualizes the application. Lastly, the PEP can also handle basic XML threats by providing schema validation, wsdl validation of incoming SOAP messages, XML structure analysis (e.g. XML node depth), etc. For more information on the PEP, please refer to [17] in these proceedings.

3.4 Policy Decision Point

The role of the Policy Decision Point (PDP) is to assist services in their access control. A service can use an associated PDP to determine whether a particular access to the service should be allowed or not. The PDP is policy-based: is based on XACML 3 with some extensions for handling delegation and obligations. For more information on the PDP, please refer to [17] in these proceedings.

4 The Business Case: on-line game application

The software components presented are arranged together, adopted and validated in a concrete business experiment of the BEinGRID project, the BE09, whose goal is to develop a Virtual Hosting Environment (VHE) for on-line game provision.

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 a typical scenario, a number of host providers offer hosting resources to the Application Providers for deploying and running their applications, which are then "virtualized" with the use of middleware services for managing non-functional aspects of the application, and are transparently exposed to the end user via a single VHE.

With the above in mind, the aim of this business experiment is to improve flexibility, dynamism and performance of the game application exposure and execution. Current gaming platforms, in fact, are very static in nature, with dedicated game servers. As such, the platforms experience extreme peaks and lows in demand, due to the period of the day or week, and ongoing gaming activity. This causes very low utilization of dedicated gaming servers, and therefore high cost of initial investment and maintenance.

The approach taken through the use of VHE is to make available infrastructure services for security, community management and virtualisation that can be used by various service providers, allowing them to link with each other. This is achieved via a generic "business-to-business gateway" component (see Figure 3).

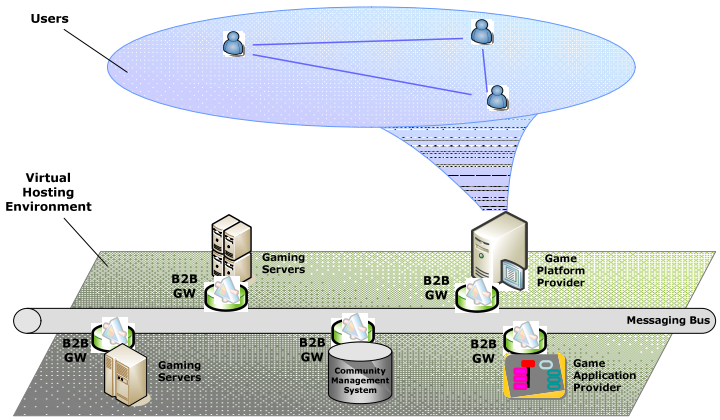

Figure 3: VHE applied to the on line gaming application

In this scenario, the game application provider deploys its gaming application onto two different execution environments (gaming servers), owned by different host providers. The game platform provider, who wants to offer the game to an end user, discovers gaming servers and creates business relationships with them, and also with a separate service provider who offers a system for community management (of gaming clans, tournaments, advanced statistics). Through use of the VHE, these various services are offered transparently to an end user, including the game platform provider's ability to perform the load balancing and server selection based on the defined SLAs

The VHE developed in this business experiment consists of a network of B2B service gateways integrated with common capabilities for B2B trust federation, identity management, access control, SLA management, accounting and monitoring, as well as application service and resource virtualisation. The B2B gateway functionality is complemented by a federated messaging bus and community management services that facilitate the establishment of B2B collaborations (e.g. in the form of Virtual Organisations).

5 Main results

The scenario presented above is clearly a B2B collaborative scenario which foresees the federation of several Service and Game providers. In this scenario we have done preliminary validation of the capabilities of the VO set-up and the triplet STS-PDP-PEP.

With respect to the VO Set-up, the purpose of our tests has been to assess the following functionalities required in the VO formation phase: (*i*) Discovery of potential members on the basis of the capabilities they can offer to the VO, (*ii*) Invite potential member to join the VO, (*iii*) Start the secure federation process, and (*iv*) Publish VO members, after their acceptance of the invitation

Our scenario presumes that each potential member of the VO has advertised to the rest of the world its capabilities. This is done, in our scenario, off-line by the Game Provider Administrator. The Game Provider presents a single point of access and a two level hierarchy of registries to publish its business capabilities. One on each hosts of the provider domain there is an Host Instance Registry. One on the provider Gateway, there is a Gateway Instance Registry

The Game Provider has a business relationship with an entity providing a general catalogue and advertises to the rest of the world its capabilities via the catalogue.

The following picture graphically shows the situation.

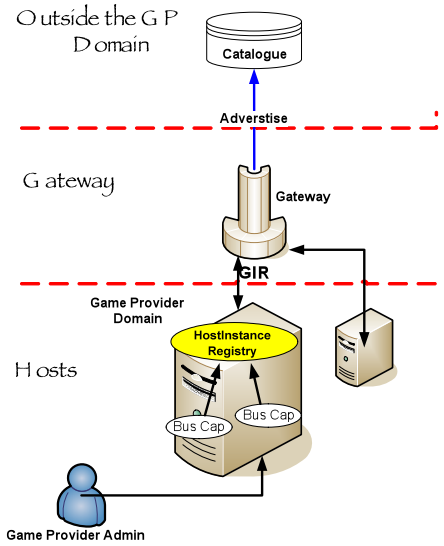

Figure 5: Game advertising

Apart from the registry management part of the VO set-up component, that involves traditional publish / update operations, our tests have been mainly focused on the secure federation of VO members.

Therefore, a focus from a security perspective was the governance and deployment of security infrastructure services including the PEP, PDP, and STS. The experiment allowed to verify that all three components could be centrally managed and configured in a coherent way. Additionally, there has been significant research into further security components, namely XML security gateways (advanced PEPs), and as a result the experiment has been looking at different vendors' solutions.

From a methodological point of view, we have assessed the added-value of the proposed model for federation of administrative domains with respect to the current state of the art. The proposed model allows, for example, a single administrative domain to federate just a specific capability. This allows a more fine grained approach to resources and services federation more suitable for business applications with respect to the models proposed in the eScience community.

6 Business benefits

The validation of the software components in a real business scenario allowed the authors to assess the following business benefits:

Identity and Federation management services: These allow, on the one hand, managing 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-cycled 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.

- 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 some middleware vendor or instead of departing in expensive product integration projects that give them identity provision and federation, at a very high cost, for the specific application at hand.

Flexible, context-aware & adaptive security: the STS-PDP-PEP triplet can be quickly and easily configured to suit the current security situation of exposed services. If new threats are detected such as repetitive failed access attempts, the security infrastructure can reconfigure itself to further prevent such tentative and therefore minimize such risks as denial of service.

7 Conclusions

Even if in this paper we have taken a closer look to a specific experiment, the software components presented can be reused in several common contexts where there is the need to federate different administrative domain and, as evidenced, can be composed in order to address complex issues, such as the creation and management of the VHE previously described.

From a methodological point of view, we have assessed the added-value of the proposed model for federation of administrative domains with respect to the current state of the art. The proposed model allows, for example, a single administrative domain to federate just a specific capability. This allows a more fine grained approach to resources and services federation more suitable for business applications with respect to the models proposed in the eScience community.

From a technological point of view, the main issue encountered has been related to the integration of the software components in the business experiment scenarios. The software components, in fact, have been developed on top of different technologies and different implementations of WS-* specifications.

References

[1]. Foster I., Kesselman C., Tuecke S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of Supercomputer Applications, 2001, Vol. 15, No. 3, 200-222

[2]. Gamma E., Helm R., Johnson R., Vlissides J.: Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, 1995 ISBN 0201633612

[3]. A. Gaeta, M. Gaeta, A. Smith, I. Djordjevic, T. Dimitrakos, M. Colombo and S. Miranda "Design patterns for Secure Virtual Organization Management Architecture" proceeding of the First International Workshop on Security, Trust and Privacy in Grid Systems, September 17, Nice, France. Accepted for publication in a Special Issue of Future Generation Computer Systems Elsevier B.V. Journal

[4]. Virtual Organization Membership Service, http://hep-project-grid-scg.web.cern.ch/hep-project-grid-scg/voms.html

[5]. GridShib, http://gridshib.globus.org/

[6]. BEinGRID project website: http://www.beingrid.eu

[7]. Gridipedia Web Site http://www.gridipedia.com

[8]. Secure Federation Design Pattern http://www.gridipedia.com/341.html

[9]. Security Design patterns http://www.gridipedia.com/262.html

[10]. SLA Design patterns http://www.gridipedia.com/204.html

[11]. BEinGRID D3.03.1: BE03 requirements description, BEinGRID Deliverable

[12]. BEinGRID D3.05.1: BE05 requirements description, BEinGRID Deliverable

[13]. BEinGRID D3.09.1: BE09 requirements description, BEinGRID Deliverable

[14]. BEinGRID D3.14.1: BE14 requirements description, BEinGRID Deliverable

[15]. BEinGRID D3.15.1: BE15 requirements description, BEinGRID Deliverable

[16]. TrustCom project: www.eu-trustcom.com/

[17]. Common Capabilities for Trust & Security in Service Oriented Infrastructures

[18]. Christian Geuer-Pollmann. "How to Make a Federation Manageable". In Proc. of "Communications and Multimedia Security" 9th IFIP TC-6 TC-11 International Conference, CMS 2005, Salzburg, Austria, Sept. 19 – 21, 2005.