Composable Services Architecture for Dynamically Configurable Virtualised Infrastructure Services Provisioning

Yuri Demchenko
University of Amsterdam
y.demchenko@uva.nl
Cees de Laat
University of Amsterdam
delaat@uva.nl

Diego R. Lopez
RedIRIS
diego.lopez@rediris.es
Joan A. García-Espín
I2CAT Foundation
joan.antoni.garcia@i2cat.net

Abstract

Effective use of existing network and IT infrastructure can be achieved by providing combined network and IT resources on-demand as infrastructure services that are capable of supporting complex scientific experiments, technological processes, and collaborative groups of researchers and applications. The paper provides a short overview of the existing standards and technologies and refers to the on-going projects and experiences in developing architectural frameworks and tools for on-demand network and Grid/Cloud services provisioning. The paper proposes the Composable Services Architecture (CSA) that is intended to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services. The paper discusses another important component of the proposed architecture the CSA Service Delivery Framework (SDF) that provides a basis for defining the whole composable services life cycle management (provisioned on-demand) and supporting infrastructure services. The proposed CSA SDF extends the existing services lifecycle management frameworks with additional stages such as "Registration and Synchronisation" and "Reservation Session Binding" that specifically target such scenarios as the provisioned resources restoration or migration/re-planning and provide a mechanism for consistent security services provisioning as an important component of the provisioned on-demand infrastructure services. The presented architecture is the result of the ongoing cooperative effort of the two EU project GEANT3 JRA3 Composable Services and GEYSERS and currently considered to be contributed to the Open Grid Forum standardisation activity.

1. Introduction

Modern e-Science applications and high-technology industry deal with large volume of data that must be stored, processed and visualised and require dedicated high-speed network infrastructure, that should be provisioned on-demand to reach all potential application scenarios. Currently large Grid projects and Cloud Computing providers use their own dedicated network infrastructure that can handle the required data throughput but typically are over-provisioned. Their network infrastructure and security model are commonly based on the traditional VPN model that spreads worldwide, provides distributed environment for running their own services geographically distributed (like Google and Amazon), and provides localised access for users and local providers. Their service delivery business model and consequently security model are typically based and governed by a Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations.

Most of Grid/Cloud usage scenarios for collaboration can benefit from combined computer/IT and network resources provisioning that besides improving performance can address such issues as application-centric manageability, consistency of the security services and becoming currently more important energy efficiency. The combined Grid/Cloud and network resources provisioning requires that a number of services and resource controlling systems interoperate at different stages of the whole provisioning process. However in current practice different systems and provisioning stages are not connected into one workflow and cannot keep the required provisioning and security context, what results in a lot of manual work and many decision points that require human involvement.

Recently, Cloud technologies [1, 2] are emerging as infrastructure services for provisioning computing and storage resources, and expectedly they will evolve into general IT resources, providing a basis for true New Generation Networks (NGN) as defined by ITU-T [3, 4]. Cloud Computing can be considered as natural evolution of the Grid Computing technologies to more open infrastructure-based services.

This paper presents the ongoing research aimed at developing an architectural framework that will address known problems in on-demand provisioning virtualised

infrastructure services that may include both computing resources (computers and storage) and transport network. The solutions for pooling, virtualising and provisioning computing resources are provided by current Grid and Cloud infrastructures. New solutions should allow the combination of IT and network resources, supporting abstraction, composition and delivery for individual collaborating user groups and applications.

The proposed Composable Services Architecture (CSA) is intended to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services. The paper also describes the CSA Service Delivery Framework (SDF) that provides a basis for defining the whole composable services life cycle management and supporting infrastructure services. The proposed SDF extends the existing services lifecycle management frameworks with additional stages such as "Registration and Synchronisation" (as part of the general services deployment process) and "Reservation Session Binding" (as part of the general services composition/reservation stage). The proposed extensions specifically target such scenarios as the provisioned resources restoration or migration/re-planning and provide a mechanism for consistent security services provisioning as a part of the provisioned on-demand infrastructure services.

The presented architecture is the result of the ongoing cooperative effort of the two EU projects GEANT3 JRA3 Composable Services [5] and GEYSERS [6] and currently considered to be contributed to the Open Grid Forum (OGF) standardisation activity. Current development is based on previous works by the authors in the framework of the EGEE and Phosphorus projects [7, 8] that have been resulted in proposing the general Complex Resource Provisioning (CRP) model [9] that includes such main stages as reservation, deployment, access, and decommissioning.

The paper is organized as follows. Section 2 analyses the typical infrastructure for e-Science applications that includes computing, storage, visualisation and their connection to network infrastructures. Section 3 provides short overview of the existing standardisation frameworks and refers to the NGN concept and its Web Services based convergence model, as defined by ITU-T and TeleManagement Forum (TMF), and discusses the paradigm shift in what relates to service provisioning in emerging Clouds computing as an infrastructure service. The section also provides a short overview of the SOA based technologies that address service delivery and lifecycle management. Section 4 presents the proposed Composable Services Architecture Section 5 describes the proposed CSA Services Delivery Framework (SDF). Section 6 provides information about the ongoing development of the GEMBus that is considered as an middleware and enabling technology for the dynamically provisioned composable services integration.

2. On-Demand Infrastructure Services Provisioning

In general, we can consider two basic use cases for on-demand infrastructure services provisioning: large scientific infrastructure and transport network infrastructure provisioning. These use cases represent the two different perspectives in developing infrastructure services – users and application developers perspective, on one side, and providers perspective, on the other side. Users are interested in uniform and simple access to the resource and the services that are exposed as Cloud/Grid resources and can be easily integrated into the scientific or business workflow. Infrastructure providers are interested in infrastructure resource pooling and virtualisation to simplify their on-demand provisioning and extend their service offering and business model to Virtual Infrastructure provisioning (see GYESERS project for details [6]).

Figure 1 illustrates the typical e-Science infrastructure that includes Grid and Cloud based computing and storage resources, instruments, control and monitoring system, visualization system, and users represented by user clients. The diagram also reflects that there may be different types of connecting network links: high-speed and low-speed which both can be permanent for the project or provisioned on-demand.

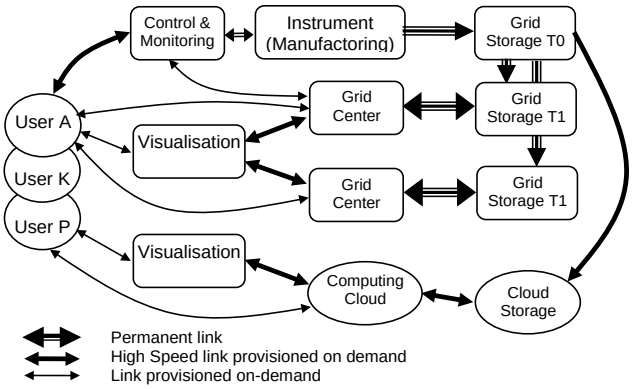

Figure 1. Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure.

Typically business relations for the provider are expressed in the SLA that defines the services provided by the provider, including security services that are provided as a part of the provider Cloud environment. The proposed/provisioned services are uniform and cannot be modified or configured by user what creates problems for their integration into the existing user infrastructure or building effective project based collaborative environment. With wider adoption of the Cloud infrastructure services and their integration into organisational IT infrastructure the demand will be

growing for dynamically configurable/manageable composable services. The solution for mentioned problems can be seen in provisioning manageable, dynamically configured services that support all stages of on-demand infrastructure services provisioning. This problem is being researched as a part of the GEANT3 JRA3 Composable Services [5].

3. Convergence Network and Computing Services in NGN and Clouds

3.1. NGN Convergence Model Using Web Services

The Next Generation Networks concept and framework (NGN) is introduced by ITU-T as a next step in creating Global Information infrastructure and provides a good basis for network and IT services convergence. The NGN principles and the general reference model specified in the ITU-T Recommendation Y.2011 [3] separate NGN services from the NGN transport network what allows for more service oriented approach in designing both transport network and network based services. Modern networking environment is characterised by integration between services and network infrastructure, increasing use of Internet protocols for inter-service communication, services "digitising", and integration with the higher level applications.

It is a natural step that NGN technology are moving to adopting SOA concepts and Web Services based services integration model to build Open Service Environment (OSE) as pre-scribed by another set of ITU-T standards defining NGN convergence model based on Web Services [10] and required NGN capabilities to support OSE [11]. Web services enabled NGN transport networks provide a native environment for integrating applications, services and resources that can be provisioned on-demand.

3.2. Paradigm Shift in Cloud Computing as Infrastructure Services

Emerging Clouds as infrastructure services suggest closer integration with the traditional network services (providing end-to-end or multi-point connectivity) and drive service delivery and security paradigms change in the general on-demand services provisioning.

The current Cloud services implement 3 basic provisioning models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1, 2]. There are many examples of the latter two models, PaaS and SaaS, can actually be built using existing SOA and Web Services or REST technologies, and there are many examples of their successful implementation and operation. However, the IaaS model if intended to provision user or operator manageable infrastructure services requires a new type of the service delivery and operation framework which is discussed in this paper. According to our analysis, existing declared IaaS implementations and providers actually realise Hardware as a Service (HaaS) model that still runs on the IaaS provider infrastructure and network [12]. Such approach doesn't provide necessary flexibility and manageability in creating user specific infrastructures that can be provisioned on demand that could be also capable of combining services from multiple providers. The problem of developing the generic model and framework for dynamically composable infrastructure services remains.

3.3. Existing Service Lifecycle Management Models

Service Oriented Architecture (SOA) [13] provides effective model and technological basis for designing virtualised dynamically configured services. It allows for better integration between business process definition with higher abstraction description languages and dynamically composed services and provides a good basis for creating composable services that should also rely on the well-defined services lifecycle management (SLM) model. Most of existing SLM frameworks and definitions are oriented on rather traditional human-driven services development and management. Dynamically provisioned and re-configured services will require re-thinking of existing models and proposing new security mechanisms at each stage of the typical provisioning process.

The Open Group Service Integration Maturity Model (OSIMM) [14] provides a good tool for evaluation and development of the SOA compliant services and defines security services as a basic services that according to the OSIMM model can be composed, virtualised and dynamically reconfigured. This implies more motivations to define the consistent Composable Services lifecycle management framework discussed in the paper.

To answer dynamic character of the NGN concept that adopts the SOA principles, the TeleManagement Forum (TMF) [15] proposed the Service Delivery Framework (SDF) [16]. The main lifecycle phases/stages defined by SDF include: service request, design/development, deployment, operation, decomposition.

Defining different lifecycle stages allows using different level of the services presentation and description at different stages and addressing different aspects and characteristics of the provisioned services. To ensure integrity of the service lifecycle management, the consistent services context management mechanisms should be defined and used during the whole service lifecycle. In particular case of the security services, the security services should ensure integrity/continuity of the service context management together with ensuring integrity of the security context itself. The proposed mechanisms should provide additional features to support

services state management when integrating with the generically stateless Web Services Architecture (WSA) based services [17, 18].

4. The Composable Services Architecture

The proposed CSA provides a framework for the design and operation of the composite/complex services provisioned on-demand. It is based on the component services virtualisation, which in its own turn is based on the logical abstraction of the (physical) component services and their dynamic composition. Composite services may also use the Orchestration service provisioned as a CSA infrastructure service to operate composite service specific workflow.

4.1. Architecture Layers

The CSA adopts the general Web Services layering model to address requirement of the vertical and horizontal interoperability and integration to allow working in multidomain environment [17] (see Figure 2 below).

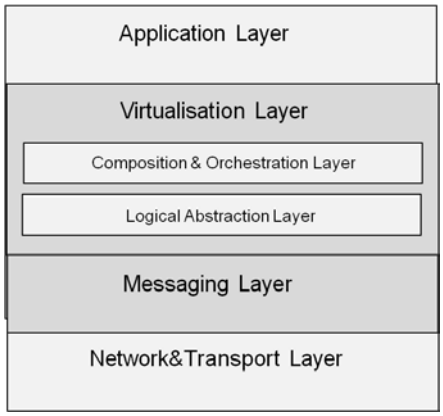

Figure 2. Composable Service Architecture Layers.

The following functional layers are defined:
Networking Layer: this layer provides a possibility to apply technologies typical for distributed enterprise applications, such as VPN
Transport Layer: this layer may define specific for service communication functionality such as transport layer security (using TLS/SSL protocols), assigning service (types) to specific ports, etc.
Messaging Layer: this layer defines message handling functionality such as message routing, message format transformation, etc.
Virtualisation Layer (that actually consists of the Logical Abstraction Layer and the Composition and Orchestration layer): this layer provides functionality to compose services and supports their interaction (e.g. with workflows).
Application Layer: this layer represents applications, where the major goal is application related data handling.
Security services are applied at multiple layers to ensure consistent security. Management functions are also present at all layers and can be seen as the management plane.

4.2. Main CSA Functional Components

Figure 3 shows that major functional components of the proposed CSA and their interaction. The central part of the architecture is the CSA middleware that should ensure smooth service operation during all stages of the composable services lifecycle.
Composable Services Middleware (CSA-MW) provides common interaction environment for both (physical) component services and complex/composite services, built with them. Besides exchanging messages, CSA-MW also contains/provides a set of basic/general infrastructure services required to support reliable and secure (composite) services delivery and operation:

- Service Lifecycle Metadata Service (MD SLC) that stores the services metadata and in particular the services state and the provisioning session context.
- Registry service that contains information about all component services and dynamically created composite services. The Registry should support automatic services registration.
- Logging service that can be also combined with the monitoring service.
- Middleware Security services that ensure secure operation of the CSA/middleware.

Note, both logging and security services can be also provided as component services that can be composed with other services in a regular way.
The CSA defines also Logical Abstraction Layer for component services and resources that is necessary part of creating services pool and virtualisation. Another functional layer is the Services Composition layer that allows presentation of the composed/composite services as regular services to the consumer.
The Control and Management plane provides necessary functionality for managing composed services during their normal operation. It may include Orchestration service to coordinate component services operation, in a simple case it may be standard workflow management system.
CSA defines a special adaptation layer to support dynamically provisioned Control and Management plane interaction with the component services which to be included into the CSA infrastructure must implement adaptation layer interfaces that are capable of supporting major CSA provisioning stages, in particular, service identification, services configuration and metadata including security context, and provisioning session management.

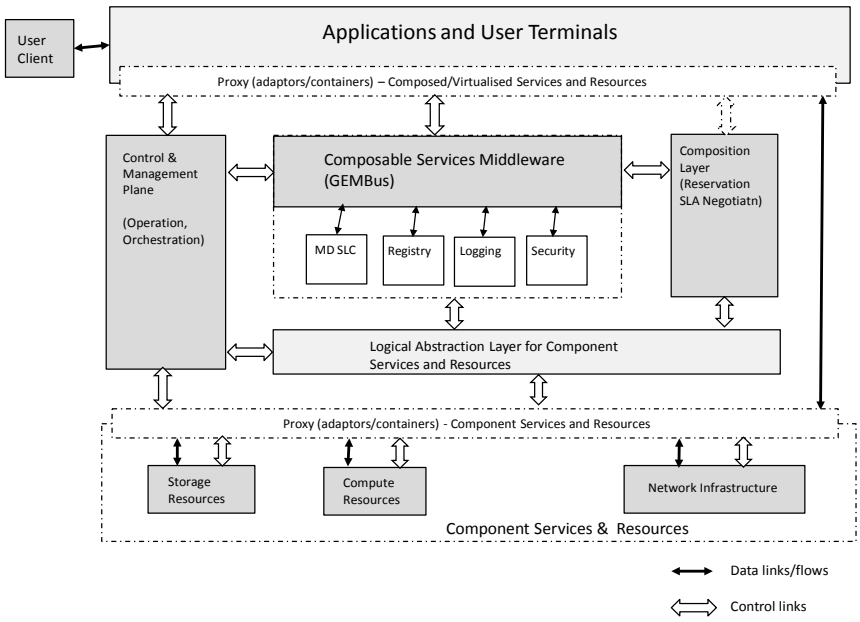

Figure 3. Composable Service Architecture and main functional components.

5. CSA Service Delivery Framework

5.1 SDF Workflow

Figure 4 illustrates the main service provisioning or delivery stages:

Service Request (including SLA negotiation). The SLA can describe QoS and security requirements of the negotiated infrastructure service along with information that facilitates authentication of service requests from users. This stage also includes generation of the Global Reservation ID (GRI) that will serve as a provisioning session identifier and will bind all other stages and related security context.

Composition/Reservation that also includes **Reservation Session Binding** with GRI what provides support for complex reservation process in potentially multidomain multi-provider environment. This stage may require access control and SLA/policy enforcement.

Deployment, including services **Registration and Synchronisation**. Deployment stage begins after all component resources have been reserved and includes distribution of the common composed service context (including security context) and binding the reserved resources or services to the GRI as a common provisioning session ID. The Registration and Synchronisation stage (that however can be considered as optional) specifically targets possible scenarios with the provisioned services migration or re-planning. In a simple case, the Registration stage binds the local resource or hosting platform run-time process ID to the GRI as a provisioning session ID.

Operation (including Monitoring). This is the main operational stage of the provisioned on demand composable services. Monitoring is an important functionality of this stage to ensure service availability and secure operation, including SLA enforcement.

Decommissioning stage ensures that all sessions are terminated, data are cleaned up and session security context is recycled. Decommissioning stage can also provide information to or initiate services usage accounting.

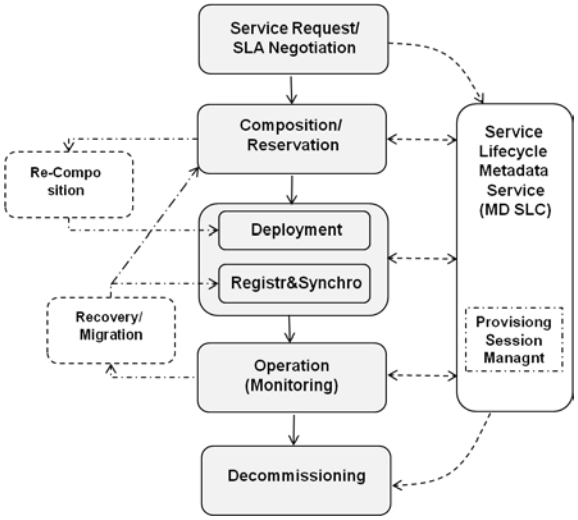

Figure 4. On-demand Composable Services Provisioning Workflow.

The two additional (sub-)stages can be initiated from the Operation stage and/or based on the running composed service or component services state, such as their availability or failure:
Re-composition or **Re-planning** that should allow incremental infrastructure changes.
Recovery/Migration can be initiated both the user and the provider. This process can use MD-SLC to initiate full or partial resources re-synchronisation, it may also require re-composition.

5.2. Infrastructure services to support CSA SDF

Implementation of the proposed SDF requires a number of special Infrastructure Support Services (ISS) to support consistent (on-demand) provisioned services lifecycle management (similar to mentioned above TMF SDF [16]) that can be implemented as a part of the CSA middleware. The following services are essential to support consistent Service Lifecycle Management:

- Service Repository or Service Registry that supports services registration and discovery
- Service Lifecycle Metadata Repository (MD SLC as shown on Figure 3) that keeps the services metadata during the whole services lifecycle that include services properties, services configuration information and services state;
- Service and Resource Monitor, additional functionality that can be implemented as a part of the CSA middleware and provides information about services and resources state and usage.

6. CSA Implementation Suggestions

6.1. GEMBus as a Framework for Enabling Composable Services

GÉANT Multi-domain service Bus (GEMBus) is being developed as a middleware for Composable Services in the framework of GÉANT3 project that creates a new generation of the pan-European academic and research network GÉANT [19]. GEMBus incorporates the SOA services management paradigm in on-demand service provisioning. The Composable services architecture will span over different service interaction, from the infrastructure up to application elements and will provide functionality to define, discover, access and combine services in the GÉANT environment. The GEMBus is built upon the industry accepted the Enterprise Service Bus (ESB) [20] and will extend it with the necessary functional components and design pattern to support multidomain services and applications.
The goal of GEMBus is to establish seamless access to the network infrastructure and the services deployed upon it, using direct collaboration between network and applications, and therefore providing more complex community-oriented services through their composition.
Figure 5 illustrates the suggested GEMBus architecture. GEMBus infrastructure includes three main groups of functionalities:

- GEMBus Messaging Infrastructure (GMI) that includes, first of all, messaging backbone and other message handling supporting services such as message routing, configuration services, secure messaging, event handler/interceptors. The GMI is built on and extends the generic Enterprise Service Bus (ESB) functionality to support dynamically configured multidomain services as defined by GEMBus.
- GEMBus infrastructure services that support reliable and secure composable services operation and the whole services provisioning process. These include such services as Composition, Orchestration, Security, and the also important Lifecycle Metadata Service, which are provided by the GEMBus environment/framework itself.
- Component services, although typically provided by independent parties, need to implement special GEMBus adaptors or use special "plug-in sockets" that allow their integration into the GEMBus/CSA infrastructure.

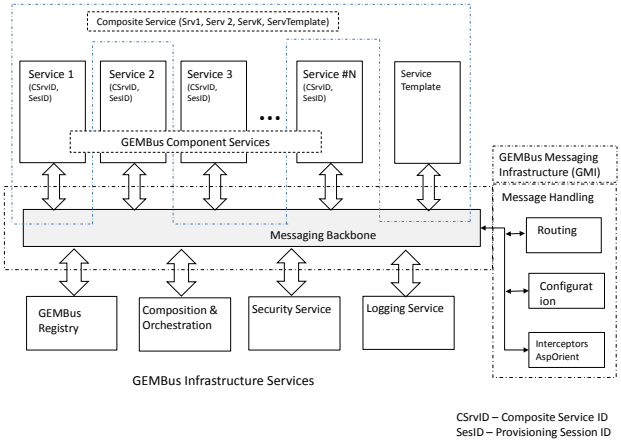

Figure 5. GEMBus infrastructure, including component services, service template, infrastructure services, and core message-processing services

The following issues have been identified to enable GEMBus operation in the multidomain heterogeneous service provisioning environment:

- Service registries supporting service registration and discovery. Registries are considered as an important component to allow cross-domain heterogeneous services integration and metadata management during the whole services lifecycle.

- Security, access control, and logging should provide consistent services and security context management during the whole provisioned services lifecycle.
- Service Composition and Orchestration models and mechanisms should allow integration with the higher level scientific or business workflow.
- Messaging infrastructure should support both SOAP-based and RESTful (conforming to Representational State Transfer (REST) architecture) services [21].

Figure 6 illustrates two examples of the composite services that are composed of four component services. In the second case the composite service contains a special Frontend service that is created of the corresponding service template that should be available for specific kind of applications. Examples of such services templates can be a user terminal (or rich user client), or a visualisation service. Requiring the GEMBus framework or toolkit to provide a number of typical service templates will provide more flexibility in delivery/provisioning composite services.

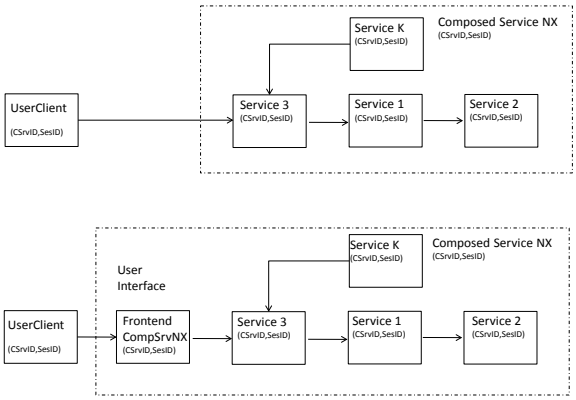

Figure 6. Example composite service composed of services Service 1, Service 2, Service 3, Service 4.

6.2. The GMI Architecture

The GEMBus Messaging Infrastructure provides necessary messages exchange environment to enable GEMBus and CSA operation.

Figure 7 illustrates the GMI functional diagram and interaction between main functional components. The diagram is presented in a such way that will allow maximum re-use of existing ESB frameworks design and achieve required GMI functionality by adding new pluggable modules or providing appropriate configuration information.

The following major structural/functional GMI components are defined:

- Message Processor/Handler
- Services interface/adapters
- Format transformation/translators/mapping
- Message/Services context handler (including communication and processes sessions support)
- Aspect based interceptors
- Configuration Manager
- Dynamic routing module (Resolver & Router)
- Events manager
- Logging facility
- Registry – to support/provide services configuration/orchestration information

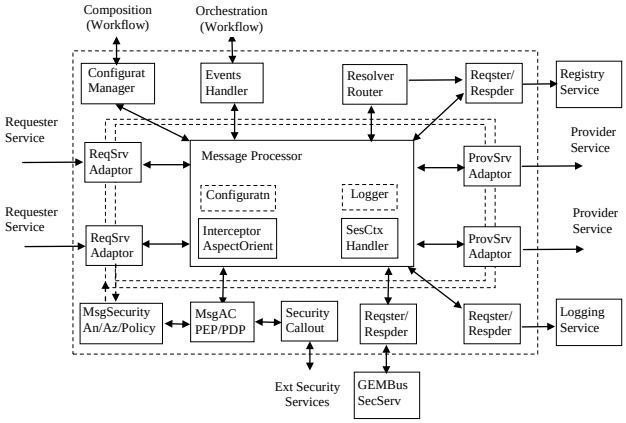

Figure 7. Main GMI functional components.

Different types of message exchange may require different functionality from the GMI:

- Regular SOAP messages having regular header and body; typical examples of these kind of messages are job submissions that have a regular header and contain a short Job description in the body
- Signaling messages are primarily used for service interactions and protocol signaling. Message information is contained in the header. These messages may contain a small or empty payload in the body
- SOAP messages with attachment that are primarily used for data communication
- Messages used as a container for routing/tunneling one or more other messages

7. Summary and future developments

This paper presents the ongoing research on developing architecture and framework for dynamically provisioned and reconfigurable infrastructure services to support modern e-Science and high-technology industry applications that require both high-performance computing resources (provisioned as Grids or Clouds) and high-speed dedicated transport network.

The paper discusses conceptual issues in on-demand provisioning infrastructure services and provides practical suggestions for provisioning consistent security services as a part of the general service provisioning.

The paper refers to the basic concepts in NGN as defined by ITU-T and TMF that includes SOA approach and Web Services based convergence model that presents a native environment for emerging Cloud technologies integration. The paper also discusses the security paradigm shift when using Clouds for on-demand data processing in scientific or industry applications that concerns data security.

The paper proposes the Composable Services Architecture (CSA) that is intended to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services.

The paper analyses existing frameworks for dynamically composed services lifecycle management and proposes the CSA Service Delivery Framework that extends the SDF defined by TeleManagement Forum to address secure composable services operation and integration in heterogeneous multidomain environment. The proposed SDF includes such additional stages such as "Registration and Synchronisation" (as part of the general services deployment process) and "Reservation Session Binding" (as part of the general services composition/reservation stage). The proposed extensions specifically target such scenarios as the provisioned resources restoration or migration/re-planning and provide a mechanism for consistent security services provisioning as an important component of the provisioned on-demand infrastructure services.

The proposed CSA is currently being implemented in the framework of the GEANT3 Project as an architectural component of the GEANT Multidomain service bus (GEMBus). The GEMBus extends the industry adopted Enterprise Service Bus (ESB) technology with the additional functionality to support multidomain services provisioning. The GEMBus infrastructure intended to allow dynamic composition of the infrastructure services to support collaboration of the distributed groups of researchers.

The concepts and solutions presented in this paper are intended tol be offered as a contribution to the prospective Open Grid Forum (OGF) Research Group on On-Demand Infrastructure Services Provisioning (ISOD-RG) and the authors were active contributors to the seria of Workshops and BoF at OGF28 [22].

The authors believe that concepts proposed in this paper will provide a good basis for the further discussion among researchers about defining an architecture for dynamically configured virtualised infrastructure services as a part of the Clouds IaaS model.

8. References

[1] GFD.150 Using Clouds to Provide Grids Higher-Levels of Abstraction and Explicit Support for Usage Modes. [Online] http://www.ogf.org/documents/GFD.150.pdf

[2] NIST Definition of Cloud Computing v15. [Online] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[3] T-REC Y.2011 General principles and general reference model for Next Generation Networks, ITU-T Recommendation, October 2004

[4] T-REC Y.2012 Functional requirements and architecture of the NGN release 1, September 2006

[5] GEANT Project. http://www.geant.net/pages/home.aspx

[6] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project) - http://www.geysers.eu/

[7] Demchenko, Y., M. Cristea, C. de Laat, E. Haleplidis, Authorisation Infrastructure for On-Demand Grid and Network Resource Provisioning, Proc. 3rd Intl ICST Conference on Networks for Grid Applications (GridNets 2009), Athens, Greece, 8-9 Sept 2009. ISBN: 978-963-9799-63-9

[8] Enabling Grid from E-sciencE (EGEE Project). [Online]. http://www.eu-egee.org/

[9] Phosphorus Project. [Online]. Available: http://www.ist-phosphorus.eu/

[10] T-REC Y.2232 NGN convergence service model and scenario using web services, ITU-T Recommendation, January 2008

[11] T-REC Y.2234 Open service environment capabilities for NGN, ITU-T Recommendation, September 2008

[12] IaaS Providers. [Online] http://www.neovise.com/iaas-providers

[13] OASIS Reference Architecture Foundation for Service Oriented Architecture 1.0, Committee Draft 2, Oct. 14, 2009. http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-cd-02.pdf

[14] The Open Group Service Integration Maturity Model (OSIMM). https://www.opengroup.org/projects/osimm/uploads/40/17990/OSIMM_v0.3a.pdf

[15] TeleManagement Forum. http://www.tmforum.org/

[16] TMF Service Delivery Framework. http://www.tmforum.org /servicedeliveryframework/4664/home.html

[17] Web Services Architecture. W3C Working Group Note 11 February 2004. [Online]. Available: http://www.w3.org/TR/ws-arch/

[18] Demchenko, Y., C. de Laat, O. Koeroo, D. Groep, Re-thinking Grid Security Architecture. Proc. IEEE Fourth eScience 2008 Conference, December 7–12, 2008, Indianapolis, USA. Pp. 79-86. ISBN 978-0-7695-3535-7 / ISBN 978-1-4244-3380-3.

[19] Deliverable DJ3.3.1: Composable Network Services use cases. GEANT3 Project Deliverable. January 11, 2010. http://www.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-09-198-DJ3_3_1_Composable_Network_Services_use_cases.pdf

[20] Chappell, D., "Enterprise service bus", O'Reilly, June 2004. 247 pp.

[21] Pautasso, C., O.Zimmermann, F.Leymann, "RESTful Web Services vs. Big Web Services: Making the Right Architectural Decision", 17th International World Wide Web Conference (WWW2008), Beijing, China.

[22] On-Demand Infrastructure Services Provisioning BoF (ISOD BoF), OGF28 meeting, 15 March 2010, Munich. http://www.gridforum.org/gf/event_schedule/index.php?id=1961