On-Demand Provisioning of Cloud and Grid based Infrastructure Services for Collaborative Projects and Groups

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

Jeroen Van der Ham
University of Amsterdam
vdham@uva.nl
Mattijs Ghijsen
University of Amsterdam
m.ghijsen@uva.nl

Vladimir Yakovenko
Google Inc.
vovik@google.com
Mihai Cristea
University of Amsterdam
m.l.cristea@uva.nl

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 technological processes, scientific experiments, and collaborative groups of researchers and applications. This paper provides a short overview of existing standards and technologies and refers to ongoing projects. We also describe experiences in developing an architectural framework and tools for combined on-demand network and Grid/Cloud service provisioning. The paper proposes an architectural framework for on-demand infrastructure service provisioning comprising of three main components: the Composable Services Architecture (CSA) that intends to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services; the Infrastructure Services Modeling Framework (ISMF) that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring; and the Service Delivery Framework (SDF) that provides a basis for defining the whole composable services life cycle management and supporting infrastructure services. We discuss implementation suggestions for the defined architectural components and provides information about the ongoing developments of the GEMBus which is considered as a middleware framework for CSA.

KEYWORDS: Cloud Computing, Infrastructure as a Service (IaaS), On-Demand Infrastructure Services Provisioning, Composable Services Architecture, Infrastructure Virtualisation.

1. INTRODUCTION

Modern e-Science and high-technology industry require high-performance infrastructures to handle large volumes of data and support complex scientific applications and technological processes. The dynamicity of projects and collaborative group environments require that such an infrastructure is provisioned on-demand and capable of dynamic (re)configuration. Currently available e-Science/research infrastructures are mostly available on Grid, which are in Europe coordinated by the European Grid Initiative (EGI) [1]. Future research infrastructures will inevitably evolve in the direction of Cloud resources and will combine Grid and Cloud resources.
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. This creates a distributed environment for running geographically distributed services (like Google and Amazon), and provides localised access for users and providers. Their service delivery business model and security model are typically governed by a Service Level Agreement (SLA) , which in general defines mutual expectations and obligations for both user and provider.

Most Grid/Cloud usage scenarios for collaboration can benefit from combined computing and network resource provisioning. Besides improving performance, this can also address issues such as application-centric manageability, security service consistency and energy efficiency, which is becoming more and more important. The combined Grid/Cloud and network resource provisioning requires that a number of services and resource controlling systems interoperate at different stages of the whole provisioning process.

Recently, Cloud technologies [2, 3] are emerging as infrastructure services for provisioning computing and storage resources, and gradually evolving into the general IT resources provisioning. Cloud Computing can be considered as natural evolution of the Grid Computing technologies to more open infrastructure-based services. Clouds "elasticity" brings a positive paradigm shift in the relation from sizing a problem to the problem-solving infrastructure towards sizing the infrastructure to the problem [4].

The current Cloud services implement three basic provisioning models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are many examples of the latter two models, PaaS and SaaS, which are typically built using existing SOA and Web Services or REST technologies. However, the IaaS model requires a new type of the service delivery and operation framework, when provisioning manageable infrastructure services.

This paper presents the ongoing research aimed at developing an architectural framework that will address known problems in on-demand provisioning of virtualised infrastructure services that may include both computing and network resources. 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 architectural framework for on-demand infrastructure services provisioning comprises of the three main components: the Composable Services Architecture (CSA) that intends to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services; the Infrastructure Services Modeling Framework (ISMF) that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring; the 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 "Reservation Session Binding" (as part of the general services composition/reservation stage) and "Registration and Synchronisation" (as part of the general services deployment process). The proposed extensions specifically target scenarios such 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 a result of an ongoing cooperative effort between two EU projects: GEANT3 JRA3 Composable Services [5] and GEYSERS [6], which aims to develop a generic architecture for Cloud Infrastructure as a Service (IaaS) provisioning model, allowing use and integration of other Cloud provisioning models for individual resource virtualisation.

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. This section also proposes an abstract model that illustrates the main stages, actors and supporting infrastructure components for on-demand provisioning infrastructure services. Section 3 provides a short description of the functionality of the Infrastructure Services Modeling Framework. Section 4 presents the Composable Services Architecture, and section 5 describes the proposed Services Delivery Framework. Section 6 provides implementation suggestions and refers to the ongoing development of the GEMBus that is considered as a middleware and enabling technology for the dynamically provisioned composable services integration. Section 7 discusses security issues in provisioning infrastructure services on-demand.

2. ON-DEMAND INFRASTRUCTURE SERVICES PROVISIONING

2.1 General use-cases

The two basic use-cases for on-demand infrastructure service provisioning can be considered: large scientific infrastructures and network infrastructure provisioning. These use-cases represent the two different perspectives in developing infrastructure services – the user and application developer perspective on one side, and the provider 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 workflows. 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.

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.

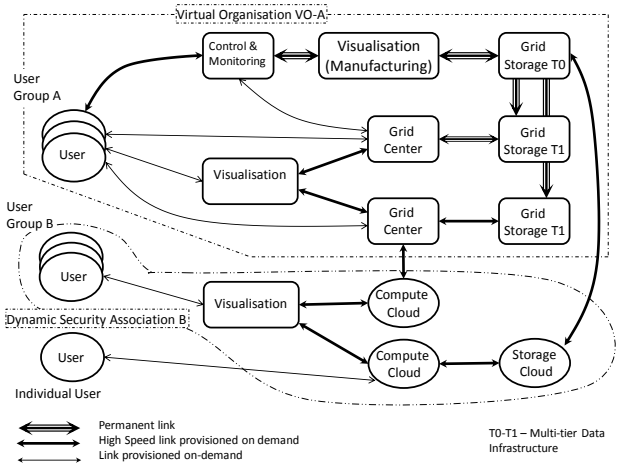

Figure 1. Components of the typical e-Science infrastructure involving multi-domain and multi-tier Grid/Cloud resources and network infrastructure.

The figure also illustrates a typical use-case of a high-performance infrastructure, which is used by two or more cooperative research groups in different locations. In order to complete their task (e.g. cooperative image processing and analysis) they require a number of resources and services to process raw data on distributed Grid or Cloud data centers, analyse intermediate data using specialised applications and finally deliver the resulting data to the scientists. This use-case includes all basic components of the typical e-Science research process: data collection, initial data mining and filtering, analysis with specialised scientific applications, and finally presentation and visualisation to the users.

2.2. Abstract model

Figure 2 below illustrates the abstraction of the typical project or group oriented Virtual Infrastructure (VI) provisioning process that includes both computing resources and supporting network that commonly referred as infrastructure services. The figure also shows the main actors involved into this process, such as Physical Infrastructure Provider (PIP), Virtual Infrastructure Provider (VIP), Virtual Infrastructure Operator (VIO).

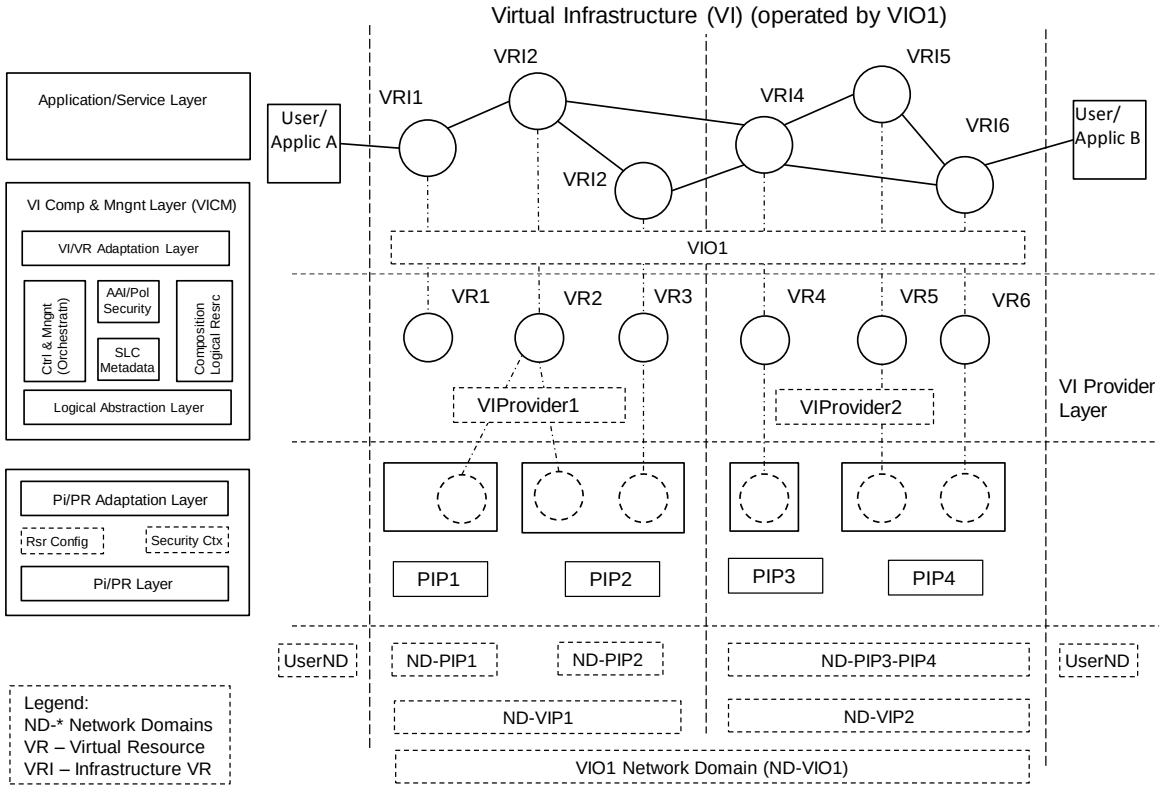

Figure 2. Main actors, functional layers and processes in on-demand infrastructure services provisioning.

The required supporting infrastructure services are depictured on the left side of the picture and includes functional components and services used to support normal operation of all mentioned actors. The Virtual Infrastructure Composition and Management (VICM) layer includes the Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper Application layer. VICM related functionality is described below as related to the proposed Composable Services Architecture (CSA).

Physical Resources (PR), including IT resources and network, are provided by Physical Infrastructure Providers (PIP). In order to be included into VI composition and provisioning by the VIP they need to be abstracted to Logical Resource (LR) that will undergo a number of abstract transformations including possibly interactive negotiation with the PIP. The composed VI need to be deployed to the PIP which will create virtualised physical resources (VPR) that may be a part, a pool, or a combination of the resources provided by PIP.

The deployment process includes distribution of common VI context, configuration of VPR at PIP, advance reservation and scheduling, and virtualised infrastructure services synchronization and initiation, to make them available to Application layer consumers.

The proposed architecture is a SOA (Service Oriented Architecture) [7] based and uses the same basic operation principles as widely known and used SOA frameworks. This also provides a direct mapping to the possible VICM implementation platforms such as Enterprise Services Bus (ESB) [8] or OSGi framework [9].

The infrastructure provisioning process, also referred to as Service Delivery Framework (SDF), is adopted from the TeleManagement Forum SDF [10, 11] with necessary extensions to allow dynamic services provisioning. It includes the following main stages: (1) infrastructure creation request sent to VIO or VIP that may include both required resources and network infrastructure to support distributed target user groups and/or consuming applications; (2) infrastructure planning and advance reservation; (3) infrastructure deployment including services synchronization and initiation; (4) operation stage, and (5) infrastructure decommissioning. The SDF combines in one provisioning workflow all processes that are run by different supporting systems and executed by different actors.

The abstract models allows outsourcing the provisioned VI operation to the VI Operator (VIO) who is from the user/consumer point of view provides valuable services of the required resources consolidation - both IT and networks, and takes a burden of managing the provisioned services.

The architecture provides a basis and motivates development of the generalised framework for provisioning dynamic security infrastructure, which includes Security Services Lifecycle Management model (SSLM), common security services interface (CSSI), and related security mechanisms to allow the consistency of the dynamically provisioned security services operation. The required security infrastructure should provide a common framework for operating security services at VIP and VIO layer and be integrated with PIP's legacy security services.

3. INFRASTRUCTURE SERVICES MODELING FRAMEWORK

The Infrastructure Services Modeling Framework (ISMF) provides a basis for virtualization and management of infrastructure resources, including description, discovery, modeling, composition, and monitoring. Figure 3 illustrates relations between different resource presentations along the provisioning process that can also be defined as the Virtual Resource lifecycle.

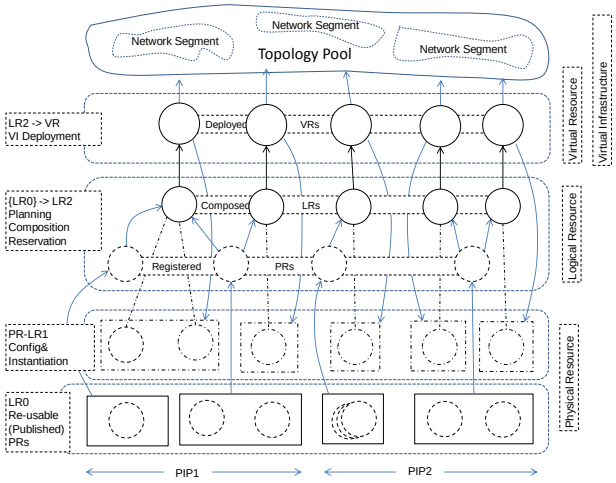

Figure 3. Relation between different resource presentations in relation to different provisioning stages (refer to Fig. 2 for the initial VI presentation).

The Physical Resource information is published by a PIP to the Registry service serving VICM and VIP. This published information describes a PR and can be called a Logical Resource (LR). Besides describing and representing a PR, the LR also defines possible (topo)logical operations on the PR, such as partitioning or aggregation. The published LR information presented in the commonly adopted form (using common data or semantic model) is then used by VICM/VIP composition

service to create the requested infrastructure using a combination of (instantiated) Virtual Resources and interconnecting them with a network infrastructure. In its own turn the network can be composed of a few network segments run by different network providers.

It is important to mention that physical and virtual resources discussed here are in fact complex software enabled systems with their own operating systems and security services. The VI provisioning process should support the smooth integration into the common federated VI security infrastructure by allowing the definition of a common access control policy. Access decisions made at the VI level should be trusted and validated at the PIP level. This can be achieved by creating dynamic security associations during the provisioning process.

The described model is being developed in the GEYSERS project [6] and aims to propose a common network and IT resource description language that will extend and combine the existing Network Description Language (NDL) [12] and the recently proposed Unified Service Description Language (USDL) [13].

4. The Composable Services Architecture

The Infrastructure as a Service provisioning is the dynamic creation of an infrastructure consisting of different types of resources together with necessary (infrastructure wide) control and management planes, all provisioned on-demand. 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 [14, 15]. The following functional layers are defined:

- **Networking and Transport Layer** allows the application of technologies typical for distributed enterprise applications, such as VPN based network layer security and TLS/SSL based transport layer security.
- **Messaging Layer** defines message-handling functionality, such as message routing, message format transformation, etc.
- **Virtualisation Layer** (a combination of the Logical Abstraction Layer and the Composition and Orchestration layer) provides functionality to compose services and supports their interaction (e.g. with workflows).
- **Application Layer** represents applications that interact with the user, 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. Control and management services related to Virtualisation Layer are defined as a part of the CSA.

4.2. Main CSA Functional Components

Figure 4 shows the major functional components of the proposed CSA and their interactions. The central part of the architecture is the CSA middleware, which should ensure smooth service operation during all stages of the composable services lifecycle.

The Composable Services Middleware (CSA-MW) provides a 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, including the lifecycle stage, the service 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 also be provided as component services that are composed of other services in a regular way.

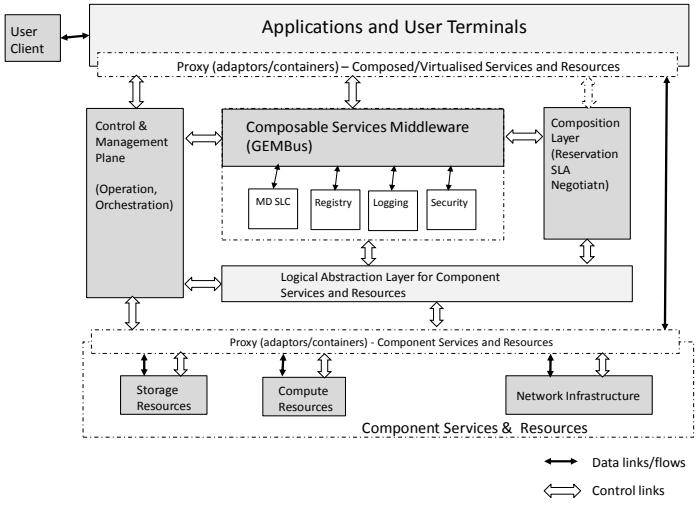

Figure 4. Composable Service Architecture and main functional components.

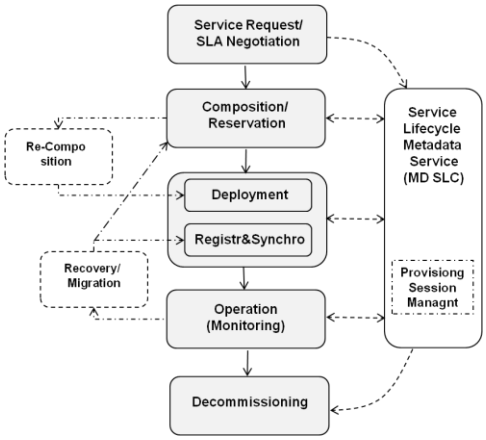

Figure 5. On-demand Composable Services Provisioning Workflow.

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 service operation. In a simple case it may be standard workflow management system.

The CSA defines a special adaptation layer to support dynamically provisioned Control and Management plane interactions with the component services. These must implement adaptation layer interfaces that are capable of supporting the major CSA provisioning stages, in particular, service identification, services configuration and metadata including security context, and provisioning session management.

5. CSA SERVICE DELIVERY FRAMEWORK (SDF)

The CSA operation relies on the well-defined services lifecycle management (SLM) model that is defined based on the TeleManagement Forum Service Delivery Framework (SDF) [10] that includes both the service delivery stages and required supporting infrastructure services.

Figure 5 illustrates the main service provisioning or delivery stages that address specific requirements of the provisioned on-demand CSA virtualised services:

Service Request Stage (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 Stage that also includes **Reservation Session Binding** with the GRI, which provides support for complex reservation processes in multi-domain multi-provider environments. This stage may require access control and SLA/policy enforcement.

Deployment Stage, including services **Registration and Synchronisation**. The 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 (which can be considered as optional) specifically targets scenarios with provisioned service 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 Stage (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 is cleaned up, and session security context is recycled. The decommissioning stage can also provide information to or initiate service usage accounting.
Two additional (sub-)stages can be initiated from the Operation stage, based on the running composed service or component services state:

Re-composition or **Re-planning Stage** should allow incremental infrastructure changes.

Recovery/Migration Stage can be initiated by the user or the provider. This process can use MD-SLC to initiate a full or partial resource re-synchronisation, it may also require re-composition.

Implementation of the proposed SDF requires a special Service Lifecycle Metadata Repository (MD SLC as shown on Figure 4) to support consistent services lifecycle management. MD SLC keeps the services metadata that include at least service state, service properties, and services configuration information.

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 [5]. GEMBus incorporates the SOA services management paradigm in on-demand service provisioning. The GEMBus is built upon the industry standard Enterprise Service Bus (ESB) [15] and will extend it with the necessary functional components and design patterns to support multi-domain 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 6 illustrates the suggested GEMBus architecture, which includes three main groups of functionalities:

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

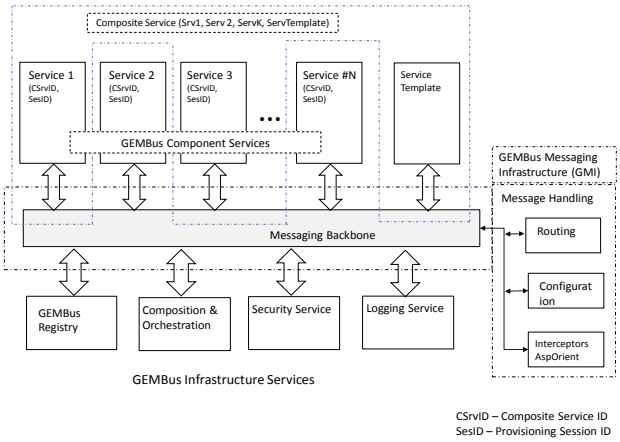

Figure 6. GEMBus infrastructure includes component services, service template, infrastructure services, and core message-processing services.

The following issues have been identified to allow GEMBus operation in the multi-domain heterogeneous service provisioning environment:

- Service registries supporting service registration and discovery. Registries are considered an important component to allow cross-domain heterogeneous service integration and metadata management during the whole service lifecycle.
- Security, access control, and logging should provide consistent service and security context management during the whole provisioned service lifecycle.
- Service Composition and Orchestration models and mechanisms should allow integration with the higher level scientific or business workflow.
- Messaging infrastructures should support both SOAP-based and RESTful (conforming to Representational State Transfer (REST) architecture) services [16].

The GEMBus and GMI in particular are built on the top of the standard Apache/Fuse messaging infrastructure that includes the following components [17, 18]:

- Fuse Message Broker (Apache ActiveMQ) messaging processor
- Fuse Mediation Router (Apache Camel) normalised message router

The GEMBus services and applications can be deployed on the standard Fuse or Apache ESB servers as component services, which can be integrated with the standard OSGi [9] and Spring [19] compliant service development frameworks and platforms such as Fuse Services Framework/Apache CXF and Fuse ESB/Apache ServiceMix.

7. CSA SECURITY INFRASTRUCTURE

Providing consistent security services in CSA and GEMBus is of primary importance due to potentially multi-provider and multi-tenant nature of Clouds IaaS environment. The CSA security infrastructure (CSA-Security) should address two aspects of the IaaS operation and dynamic security services provisioning:

- Provide a security infrastructure for secure IaaS operation, including access control and SLA and policy enforcement for all interacting roles and components in CSA, secure messaging and transport services.
- Provisioning dynamic security services, including creation and management of the dynamic security associations as part of the provisioned (composite) services or virtual infrastructures.

The first task is a traditional task in security engineering, while dynamic provisioning of managed security services remains a problem and requires additional research. In this paper we will not discuss CSA-Security in detail but refer to another paper by the authors [20], which discusses an important issue on building consistent security services for dynamically provisioned virtual infrastructures: the Security Services Lifecycle Management (SSLM). The SSLM extends the above CSA SDF service lifecycle management model and workflow with additional sub-stages and functions to bind the dynamic security context to the general provisioning session and Cloud virtualisation and hosting platform to ensure that all operations on the virtual infrastructure and user data are secured during their whole lifecycle.

CSA-Security and GEMBus should provide the following basic infrastructure security services to ensure normal operation of the virtual infrastructure:

- Access control (e.g. Authentication, Authorisation, Identity Management)
- Policy and SLA enforcement
- Data, messaging and communication security
- Additionally, auditing/logging and accounting.

CSA-Security should implement multi-layer security services including transport, messaging and application/data security, and additionally network layer security for distributed VPN based enterprise domains. Security and security services in the CSA and GEMBus design are applied at different layers and can be called from different functional components using standard/common security services interface. Security services are governed by related security policies.

8. SUMMARY AND FUTURE DEVELOPMENTS

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

The paper proposes an architectural framework for on-demand infrastructure services provisioning that comprises of the three main components: Composable Services Architecture (CSA) that intends to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services; Infrastructure Services Modeling Framework (ISMF) that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring; Service Delivery Framework (SDF), which provides a basis for defining the whole composable services life cycle management and supporting infrastructure services.

The proposed CSA is currently being implemented in 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 additional functionality to support multi-domain service provisioning. The GEMBus infrastructure intends to allow dynamic composition of the infrastructure services to support collaboration of distributed groups of researchers.

The authors believe that the concepts proposed in this paper provide a good basis for further discussion among

researchers on the definition of architectures for dynamically-configured virtualised infrastructure services as part of the Clouds IaaS model.

ACKNOWLEDGEMENT

This work is supported by the FP7 EU funded project GEANT3 (FP7-ICT-238875), and the FP7 EU funded Integrated project The Generalised Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657).

REFERENCES

[1] European Grid Infrastructure (EGI). [Online] https://www.egi.eu/
[2] NIST Definition of Cloud Computing v15. [Online] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
[3] 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
[4] CloudCom2010 Conference Panel discussion. Not published.
[5] GEANT Project. http://www.geant.net/pages/home.aspx
[6] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project) - http://www.geysers.eu/
[7] 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
[8] Chappell, D., "Enterprise service bus", O'Reilly, June 2004. 247 pp.
[9] OSGi Service Platform Release 4, Version 4.2. - http://www.osgi.org/Download/Release4V42
[10] TMF Service Delivery Framework. http://www.tmforum.org/servicedeliveryframework/4664/home.html
[11] TMF Software Enabled Services Management Solution. - http://www.tmforum.org/BestPracticesStandards/SoftwareEnabledServices/4664/Home.html
[12] J. van der Ham, F.Dijkstra, P.Grosso, R. van der Pol, A.Toonk, C. de Laat, "A distributed topology information system for optical networks based on the semantic web", Elsevier Journal on Optical Switching and Networking,Volume 5, Issues 2-3, June 2008, pp 85-93
[13] Unified Service Description Language (USDL). http://www.w3.org/2005/Incubator/usdl/
[14] Web Services Architecture. W3C Working Group Note 11 February 2004. [Online]. Available: http://www.w3.org/TR/ws-arch/
[15] Deliverable DJ3.3.2: GEMBus Architecture. GEANT3 Project Deliverable. January, 2011.
[16] 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.
[17] Fuse ESB - OSGi based ESB. - http://fusesource.com/products/enterprise-servicemix/#documentation
[18] Apache ServiceMix an Open Source ESB. - http://servicemix.apache.org/home.html
[19] Spring Security. Reference Documentation. http://static.springsource.org/spring-security/site/docs/3.1.x/reference/springsecurity-single.html
[20] Demchenko, Y., D.R. Lopez, J.A. Garcia Espin, C. de Laat, "Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning", International Workshop on Cloud Privacy, Security, Risk and Trust (CPSRT 2010), 2nd IEEE Int. Conf. on Cloud Computing Technology and Science (CloudCom2010), 30 November - 3 December 2010, Indianapolis, USA.