UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Defining Generic Architecture for Cloud Infrastructure as a Service model

Demchenko, Y.; de Laat, C.

Publication date
2011
Document Version
Final published version
Published in
Proceedings of Science

Link to publication

Citation for published version (APA):
Demchenko, Y., & de Laat, C. (2011). Defining Generic Architecture for Cloud Infrastructure as a Service model. *Proceedings of Science*, *133*, Article 115. http://pos.sissa.it/archive/conferences/133/115/ISGC%202011%20&%20OGF%2031_115.pdf

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:09 Nov 2026

PROCEEDINGS OF SCIENCE

Defining Generic Architecture for Cloud Infrastructure as a Service Model

Yuri Demchenko[1]
University of Amsterdam
Science Park 904, Amsterdam, The Netherlands
E-mail: y.demchenko@uva.nl

Cees de Laat
University of Amsterdam
Science Park 904, Amsterdam, The Netherlands
E-mail: delaat@uva.nl

Abstract

Infrastructure as a Service (IaaS) is one of the provisioning models for Clouds as defined in the NIST Clouds definition. Although widely used, current IaaS implementations and solutions doesn't have common and well defined architecture model. The paper attempts to define a generic architecture for IaaS based on current research by authors in developing novel architectural framework for Infrastructure Services On-Demand (ISOD) provisioning that allows for combined network and IT resources provisioning. The paper proposes the Composable Services Architecture (CSA) that extends the SOA based Enterprise Service Bus (ESB) architecture for dynamically configurable virtualised services. The proposed CSA includes the Services Delivery Framework (CSA SDF) as another important component that defines the services provisioning workflow and supporting infrastructure for provisioned services lifecycle management. The CSA SDF extends existing lifecycle management frameworks with additional stages such as "Registration and Synchronisation" and "Provisioning Session Binding" that target such scenarios as the provisioned services recovery or re-planning/migration and provide necessary mechanisms for consistent security services provisioning as an important component of the provisioned on-demand infrastructure. The paper also describes the GEMBus (GEANT Multidomain Bus) that is considered as a CSA middleware platform. The presented architecture is the result of the on-going cooperative effort of the two EU projects GEANT3 JRA3 Composable Services and GEYSERS.

The International Symposium on Grids and Clouds and the Open Grid Forum
Academia Sinica, Taipei, Taiwan
March 19 - 25, 2011

[1] Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike Licence.

1. Introduction

Cloud technologies [1, 2] are emerging as a common way of provisioning complex infrastructure services that may include both computing or storage resources and connecting these resources network infrastrutcure.

The current Cloud services implement 3 basic provisioning models (as defined in the NIST Special Publication 800-144 [2]): Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS suggests involving different types of resources, of which one is the network connectivity with guaranteed Quality of Service (QoS), and availability of user controlled infrastructure operation via dynamically created control and management planes/functions.

Despite rapid grow, Cloud technologies are lack of well-defined architectural framework and operational model. Current industry standardisation activity is primarily focused on functional interoperability of deployment platforms and components supporting basic usage scenarios such as applications and Virtual Machine (VM) images creation, deployment and management, services request and execution management. The currently being developed NIST Cloud Computing Reference Architecture (NIST CCRA) [3, 4] incorporates the initial Cloud definition [2] and extends it with additional definitions to ensure interoperability of the future Cloud implementations in the heterogeneous multi-provider environment. Another important document published as NIST Special Publication 800-144 provides guidelines on security and privacy issues in public Cloud Computing [5]. It is primarily oriented on Cloud customers but also provides a good evaluation framework for providers.

Typically business relations between provider and customer are expressed in the Service Level Agreement (SLA) that defines the services provided by the provider, including security services that are provided as a part of the provider Cloud environment. The offered/provided 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 for dynamically configurable/manageable composable services will be growing. 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 paper attempts to define a generic architecture for the Cloud Infrastructure as a Service provisioning model which is defined as the Composable Services Architecture (CSA). The CSA extends virtualisation and dynamic service provisioning concepts to complex infrastructure services that are composed of multiple composable component services and resources. This problem is being researched as a part of the GEANT3 JRA3 Composable Services activity [6] and GEYSERS project Logical Infrastructure Composition Layer (LICL) definition and design [7].

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 presents the proposed Composable Services Architecture and section 4 describes the proposed Services Delivery Framework (CSA SDF) that defines the on-demand service provisioning sequence and workflow. Section 5 provides information about the ongoing development of the GEMBus that is considered as a middleware and enabling technology for the dynamically provisioned composable services integration. Section 6 provides general requirements and suggestions for building consisting security in Cloud based infrastructures provisioned on-demand.

2. On-Demand Infrastructure Services 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.

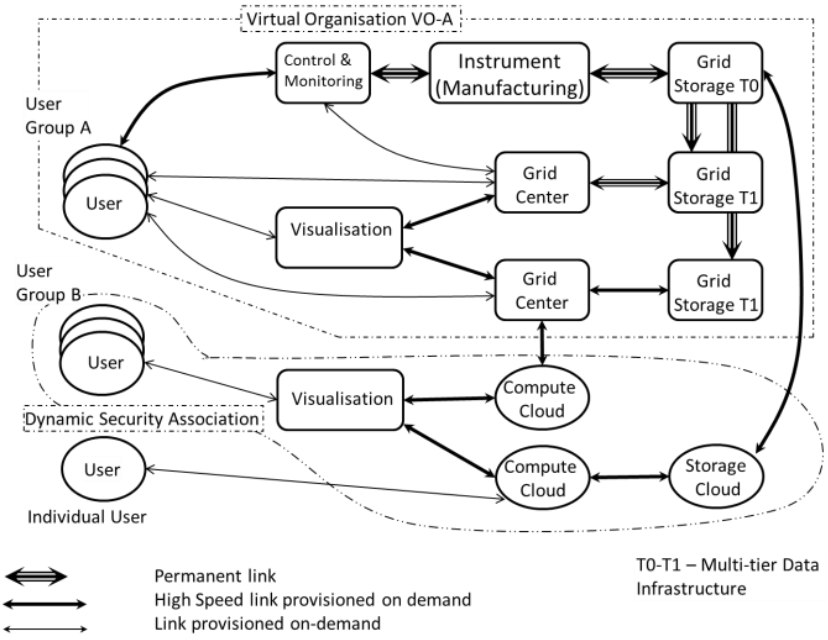

Figure 1. Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure.

The figure illustrates possible different relations between users/actors in Clouds and Grids. Grid architecture is built around so-called Virtual Organisations (VO) that are defined as collaborative associations/federations of the member organisations to share complex resources which are however remaining under control and in ownership of the VO member organisations. Grids natively supports project oriented collaborative environment with sharing resources committed/donated by the VO members. Clouds are considered as a technology for provisioning complex computing resources, applications and increasingly infrastructure resources and services on-demand on the pay-per-use base.

3. The Composable Services Architecture (CSA)

The Infrastructure as a Service provisioning involves dynamic creation of infrastructure consisting of different types of resources together with necessary 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.

The proposed architecture is a SOA (Service Oriented Architecture) [8] based and uses the same basic operation principles as widely known and used SOA frameworks such as Web Services based Enterprise Services Bus (ESB) [9]. Moving from typical for network services provisioning CORBA based platform [10] allows for easier services development and simple services integration environment [11].

Figure 2 shows the 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 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.

The CSA defines 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 also 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.

The application or service middleware layer can be defined as an additional upper CSA architecture layer to provide application – infrastructure interface with the underlying virtual infrastructure provisioned by CSA, but this functionality is typically addressed by the applications provider themselves.

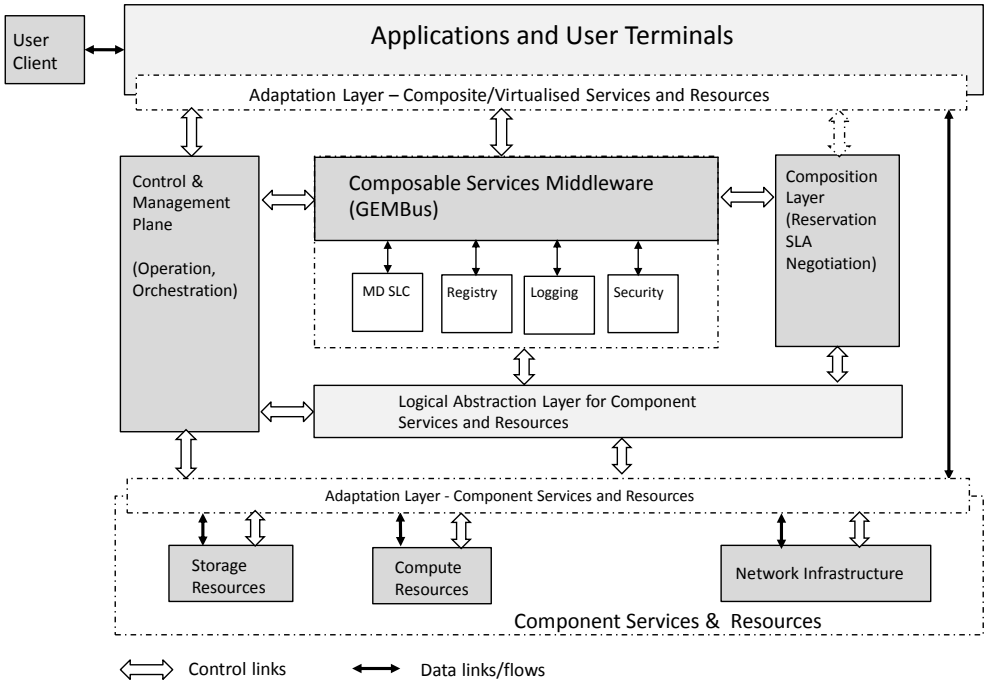

Figure 2. Composable Service Architecture and main functional components.

4. CSA Service Delivery Framework (SDF)

The proposed CSA Service Delivery Framework (CSA SDF) implements the Service Delivery Framework defined by the TeleManagement Forum (TMF) [12] and extends it with additional stages to address secure composable services operation and integration into the heterogeneous multidomain Cloud IaaS environment. Figure 3 illustrates the main service provisioning 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 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.

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.

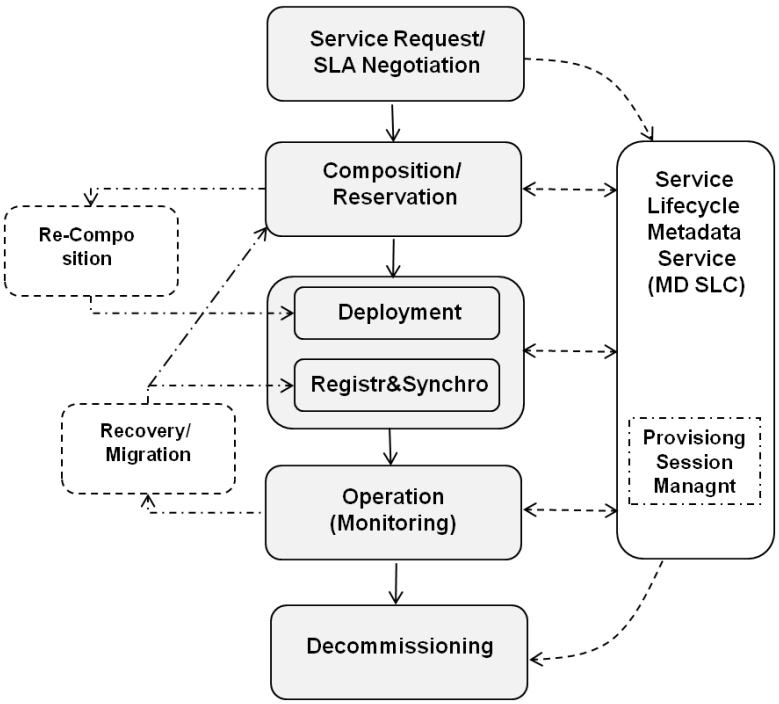

Figure 3. On-demand Composable Services Provisioning Workflow.

5. GEMBus as CSA Middleware Platform

GEANT Multidomain Bus (GEMBus) is being developed as a middleware for Composable Services [13] in the framework of the GÉANT3 project aimed for creating a new generation of the pan-European academic and research network GÉANT. The Composable Services Architecture will span over different service interactions, from the infrastructure up to

application elements and will provide functionality to define, discover, access and combine services in the GÉANT environment.

GEMBus is built upon the industry accepted the SOA based Enterprise Service Bus (ESB) [9] and extends it with the necessary functional components and design patterns to support multidomain services and applications. Figure 4 illustrates the suggested GEMBus architecture. GEMBus infrastructure includes three main groups of functionalities:

- GEMBus infrastructure services that support reliable and secure composable services operation and the whole services provisioning process. These include such services as service registries, composition and orchestration, security and access control, logging and monitoring, and the also important Lifecycle Metadata Service.
- Component services, although typically provided by independent parties, will need to implement special GEMBus adaptors or use special "plug-in sockets" that allow their integration into the GEMBus/CSA infrastructure.
- GEMBus Messaging Infrastructure (GMI) that includes the messaging backbone and other message handling services such as routing, configuration services, secure messaging, and event handler/interceptors. GMI supports both SOAP-based and RESTful services conforming to Representational State Transfer architecture (REST) [14].

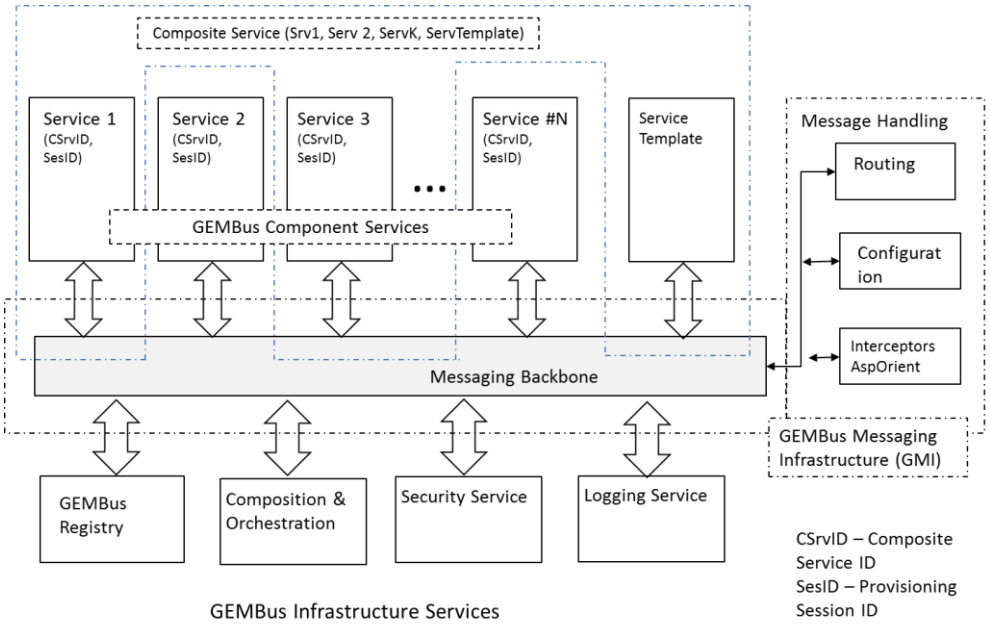

Figure 4. GEMBus infrastructure, including component services, service template, infrastructure services, and core message-processing services

The following functionalities are essential 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.

The GEMBus and GMI in particular are built on the top of the standard Apache/Fuse messaging infrastructure that includes the following components [15, 16]:

- 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 server. As component services that can be integrated with the standard OSGi [17] and Spring [18] compliant service development frameworks and platforms such as Fuse Services Framework/Apache CXF and Fuse ESB/Apache ServiceMix.

6. CSA Security Infrastructure (CSA-Security)

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 should address two aspects of the IaaS operation and dynamic security services provisioning:

- Provide 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 a part of the provisioned complex/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.

An important issue in building consistent security services for dynamically provisioned virtual infrastructures is the Security Services Lifecycle Management (SSLM) that uses the described above CSA SDF service lifecycle management model and extends it with additional sub-stages and functions to bind dynamic security context to the general provisioning session and Cloud virtualisation and hosting platform in such a way that to ensure all operations on the virtual infrastructure and user data to be secured during their whole lifecycle. It is described in details in earlier authors' paper [19].

CSA-Security and GEMBus should implement 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 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.

Security services should support the whole provisioned/composable services lifecycle and consequently support session-related security context management.

Security services can be designed as: pluggable services operating at the messaging layer; OSGi bundles that can be dynamically added as composable services to other composable services to form an instant virtual infrastructure; or exposed as Web services and be integrated with other services by means of higher level workflow management systems.

7. Summary and Future Development

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 proposes the Composable Services Architecture (CSA) that is intended to provide a conceptual and methodological framework for developing dynamically configurable virtualised 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 to be offered as a contribution to the Open Grid Forum (OGF) Research Group on On-Demand Infrastructure Services Provisioning (ISOD-RG) [20]. The authors are also actively participating in the NIST Collaboration on the defintion of the Cloud Computing Reference Architecture [21].

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.

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] GFD.150, 2009. Using Clouds to Provide Grids Higher-Levels of Abstraction and Explicit Support for Usage Modes, Open Grid Forum. [online] Available at: http://www.ogf.org/documents/GFD.150.pdf

[2] NIST SP 800-145, “A NIST definition of cloud computing”, [online] Available: http://csrc.nist.gov/publications/drafts/ 800-145/Draft-SP-800-145_cloud-definition.pdf

[3] Cloud Architecture Reference Models: A Survey. NIST CCRATWG 004 v2, January 25, 2011. [online] Available: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/Meeting4AReferenceArchtecture013111/NIST_CCRATWG_004v2_ExistentReferenceModels_01182011.pdf

[4] NIST Reference Architecture and Taxonomy. [online] Available: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy

[5] NIST SP 800-144, "Guidelines on Security and Privacy Issues in Public Cloud Computing", [online] Available: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdfGEANT3, 2010. GEANT Project. [online] Available at: http://www.geant.net/pages/home.aspx

[6] GEANT Project [website], January 20, 2011. [online] Available: http://www.geant.net/pages/home.aspx

[7] GEYSERS Project. Generalised Architecture for Dynamic Infrastructure Services, EU Project. http://www.geysers.eu/

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

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

[10] OMG CORBA®/IIOP® Specifications. [online] Available at http://www.omg.org/technology/documents/corba_spec_catalog.htm

[11] Petritsch H., "Service-Oriented Architecture (SOA) vs. Component Based Architecture". [online] Available at http://petritsch.co.at/download/SOA_vs_component_based.pdf

[12] Service Delivery Framework. TeleManagement Forum. [online]. Available at: http://www.tmforum.org /servicedeliveryframework/4664/home.html

[13] GEANT3 DJ3.3.1. Composable Network Services use cases. GEANT3 Project Deliverable. January 11, 2010. [online] Available at: http://www.geant.net/ Media_Centre/Media_Library/ Media%20Library/GN3-09-198-DJ3_3_1_ Composable_Network_Services_ use_cases.pdf

[14] 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.

[15] Fuse ESB - OSGi based ESB. [online] Available at: http://fusesource.com/products/ enterprise-servicemix/#documentation

[16] Apache ServiceMix an Open Source ESB. [online] Available at: http://servicemix.apache.org/home.html

[17] OSGi Service Platform Release 4, Version 4.2. [online] Available at: http://www.osgi.org/Download/Release4V42

[18] Spring Security. Reference Documentation. [online] Available at: http://static.springsource.org/spring-security/site/ docs/3.1.x/reference/springsecurity-single.html

[19] 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 International Conference on Cloud Computing Technology and Science (CloudCom2010), 30 November - 3 December 2010, Indianapolis, USA.

[20] OGF Infrastructure Services On-Demand Provisioning Research Group (ISOD-RG). [online] Available: http://www.gridforum.org/gf/group_info/view.php?group=ISOD-RG

[21] NIST Cloud Computing Collaboration Site. [online] Available: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/