Security Services Lifecycle Management
in On-Demand Infrastructure Services Provisioning

Yuri Demchenko, Cees de Laat
System and Network Engineering Group
University of Amsterdam
The Netherlands
e-mail: {y.demchenko, delaat}@uva.nl

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

***Abstract*—Modern e-Science and high technology industry require high-performance and complicated network and computer infrastructure to support distributed collaborating groups of researchers and applications that should be provisioned on-demand. The effective use and management of the dynamically provisioned services can be achieved by using the Service Delivery Framework (SDF) proposed by TeleManagement Forum that provides a good basis for defining the whole services life cycle management and supporting infrastructure services. The paper discusses conceptual issues, basic requirements and practical suggestions for provisioning consistent security services as a part of the general e-Science infrastructure provisioning, in particular Grid and Cloud based. The proposed Security Services Lifecycle Management (SSLM) model extends the existing frameworks with additional stages such as "Reservation Session Binding" and "Registration and Synchronisation" that specifically target such security issues as the provisioned resources restoration, upgrade or migration and provide a mechanism for remote executing environment and data protection by binding them to the session context. The paper provides a short overview of the existing standards and technologies and refers to the on-going projects and experience in developing dynamic distributed security services.**

Keywords-On-demand Infrastructure Services Provisioning, Security Services Lifecycle Management Model (SSLM), Composable Services, Security Context.

I. 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 security infrastructure is commonly based on 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.

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 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 [1, 2]. Cloud Computing can be considered as natural evolution of the Grid Computing technologies to more open infrastructure-based services. Recent research based on the first wave of Cloud Computing implementation have revealed a number of security issues both in actual service organisation, and operational and business model. The current Cloud security model is based on the assumption that the user/customer should trust the provider. This is typically governed by a Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations. However, this approach doesn't scale well with a potentially growing amount of services and users, and in particular, doesn't ensure protection against malicious users and risks related to possible Denial of Service (DoS) attacks.

This paper presents the ongoing research aimed at developing a framework that will address known problems in provisioning consistent security services for dynamically provisioned and reconfigurable infrastructure services that may include both computing resources (e.g., computers and storage, also referred to as IT resources) 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.

This development is based on the previous works by the authors that have been resulted in proposing the general Complex Resource Provisioning (CRP) model, that was successfully used for developing the Generic AAA Authorisation infrastructure (GAAA-CRP) [5, 6] for combined Grid and network resources provisioning in the framework of the EGEE and Phosphorus projects [7, 8]. The proposed GAAA-CRP authorisation infrastructure supports the main stages of the CRP process/lifecycle such as reservation, deployment, access, and decommissioning. Current research and development continue in the framework of the GÉANT3 and GEYSERS projects [9, 10] and target the development of a consistent security service infrastructure for dynamically configurable composable services.

Moving to dynamic provisioning of infrastructure services will require re-thinking the existing security frameworks and basic models to allow the integration of dynamically configurable security services with the main services at different lifecycle stages and at different service layers. The proposed research scope includes both the extension of service delivery frameworks and the design of the security services themselves.

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 refers to the Next Generation Networks (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 security in emerging Clouds computing as an infrastructure service. Section 4 provides a short overview of the SOA based technologies that address service delivery and lifecycle management. Section 5 presents the proposed Security Services Lifecycle Management model and provides suggestions about its implementation. Section 6 provides information about the ongoing development of the GEMBus that is considered as an enabling technology for the dynamically provisioned composable services integration.

II. On-Demand Infrastructure Services Provisioning

In general, we can consider two basic use cases for on-demand infrastructure services provisioning: large scientific infrastructure for collaborating user communities, and combined network and IT infrastructure services provisioning. These use cases represent the two different perspectives in developing infrastructure services – users and application developers perspective, and providers perspective. Users are interested in uniform and simple access to resources and services that are exposed as Cloud 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 [10]).

Such different points of view are also reflected in their approach to the security infrastructure architecture and design. Typically business relations for the provider are expressed in the SLA that defines the services provided by the provider. Currently, security services are provided as a part of the provider Cloud environment, they are uniform and cannot be modified or configured by user. However user concerns are originated from the potential system vulnerabilities (or even operational model weaknesses) and possible malicious activities of other users that share the same resources. With wider adoption of the Cloud infrastructure services and their integration into organisational IT infrastructure the demand will be growing for configurable/manageable security services that would allow user defined security services and policies.

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.

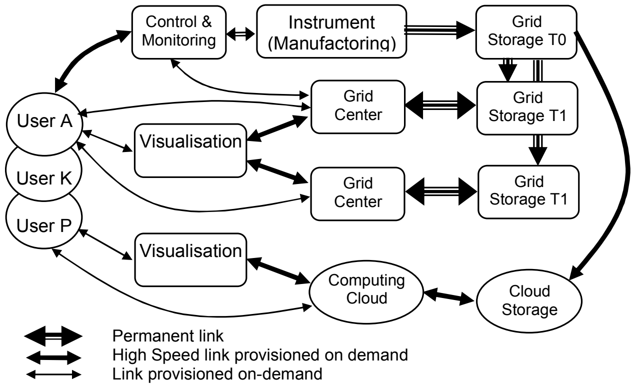

Figure 1. Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure.

With the growing complexity and dynamicity of collaborative projects and applications, they will require access to network control and management functions to optimise their performance and resources usage. Currently, transport network, even if provided as VPN, is set up statically or can only be re-configured by an network engineer. Recently developed and successfully demonstrated new generation of the on-demand Network Provisioning Systems and Network Service Planes can provide the connectivity on demand optimized for and controlled by applications [11, 12]. Moreover, efforts for seamlessly integrating computing resources and network resources provisioning on the control plane have successfully demonstrated their integration with the Grid applications [13], paving the path for integrated (IT and network) Cloud domain control.

The remaining problem in today's solutions for provisioning of multi-domain network resources is due to the traditional chain-based inter-provider trust model that requires significant manual/human involvement into infrastructure services setup and management. This trust model allows service providers to authenticate resources in own administrative or trust domain but does not allow directly authenticate and/or authorise the end users and resources that reside in different administrative domains. As a consequence, the provisioning of complex distributed resources and ensuring secure access to these resources by the users is a challenge. This problem is even more evident and important in the emerging systems that intends to support virtual infrastructures for on-demand provisioning of the combined network and IT resources that could be managed by so-called Virtual Infrastructure Providers (VIP) (see GEYSERS Project [10] for the proposed new business models description). The solution for mentioned problems can be seen in provisioning manageable, dynamically configured security services that support all stages of on-demand infrastructure services provisioning.

III. Convergence Network and Computing Services in NGN and Clouds

A. 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 is 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 [14] and required NGN capabilities to support OSE [15]. Web services enabled NGN transport networks provide a native environment for integrating applications, services and resources that can be provisioned on-demand.

B. Security Paradigm Shift in Cloud Computing as Infrastructure Service

Emerging Clouds as infrastructure services suggest closer integration with the traditional network services (providing end-to-end or multi-point connectivity) and drive security paradigm 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) [2, 16]. At this stage of the research we are considering only their common features from the security point of view and not operational specifics. We refer to some recent publications on the Clouds security that finally demonstrated convergence of the proposed security models for Clouds and provided detailed analysis of the Clouds operation [16, 17, 18].

Considering evolutional relations between Grids and Clouds, it is interesting to compare their security models. Grid security architecture is primarily based on the Virtual Organisations (VO) that are created by the cooperating organisations that share resources (which however remain in their remaining in their ownership) based on mutual agreement between VO members and common VO security policy. In Grids, VO actually acts as a federation of the users and resources that enables federated access control based on the federated trust and security model [19, 20].

Current practice in provisioning Cloud resources is mostly based on the Service Level Agreement (SLA) that also describes security measures taken by the provider but doesn't define mechanisms for checking them by users, like in case of Amazon Web Services (AWS) Cloud service [21].

In the Clouds data are sent to and processed in the environment that is not under the user or data owner control and potentially can be compromised either Clouds insiders or by other users sharing the same resource. Data/information must be secured during all processing stages – upload, process, store, stream/visualize. Policies and security requirements must be bound to the data and there should be corresponding security mechanisms in place to enforce these policies.

The security solutions and supporting infrastructure should address the following problems, mostly related to the data integrity and data processing security:

- Secure data transfer that possibly should be enforced with the data activation mechanism
- Protection of data stored on the Cloud platform
- Restore from the process failure that entails problems related to secure job/application session and data restoration.

Initial suggestions to address those problems require the consistent secure provisioning and application/job session management:

- Special session for data transfer that should also support data partitioning and run-time activation and synchronization.
- Secure job/session fail-over that should rely on the session synchronization mechanism when restoring the session.

- Session synchronization mechanisms that should protect the integrity of the remote run-time environment.

Wider Clouds adoption by industry and their integration with advanced infrastructure services will require implementing manageable security services and mechanisms for the remote control of the Cloud operational environment integrity by users.

IV. Existing Services Lifecycle Management Models

Service Oriented Architecture (SOA) [22] 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) [23] 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 Security Service Lifecycle Management (SSLM) framework which we discuss in this paper.

To answer dynamic character of the NGN concept that adopts the SOA principles, the TeleManagement Forum (TMF) [24] proposed the Service Delivery Framework (SDF) [25] as a part of their New Generation Operations Systems and Software (NGOSS) solutions framework [26]. The main lifecycle phases/stages defined by SDF are illustrates in Figure 2 (a) and 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 generally stateless Web Services Architecture (WSA) based services [27].

V. The Proposed Security Services Lifecycle Management Model

Most of the existing security lifecycle management frameworks, such as defined in the NIST Special Publication 800-14 “Generally Accepted Principles and Practices in Systems Security” [28] or Microsoft Security Development Lifecycle (SDL) [29], provide a good basis for security services development and management, but they still reflect the traditional approach to services and systems design driven by engineers force. The defined security services lifecycle includes the following typical phases: Initiation, Development and/or Acquisition, Implementation, Operation and Maintenance, and Disposal.

Figure 2 (b) illustrates the proposed Security Services Lifecycle Management (SSLM) model that reflects security services operation in generically distributed multidomain environment and their binding to the provisioned services, which SLM stages are illustrated in Figure 2 (a). The SSLM includes the following stages:

- **Service request and 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.
- **Reservation stage** that also includes **Reservation session binding** with GRI what provides support for complex reservation processes including required access control and policy enforcement.
- **Deployment stage** begins after all component resources have been reserved and includes distribution of the security context and binding the reserved resources or services to the GRI as a common provisioning session ID.
- **Registration&Synchronisation stage** (that however can be considered as a sub-stage or a part of the Deployment stage) that specifically targets possible scenarios with the provisioned services restoration in case of their failure or migration. In a simple case, the Registration stage binds the local resource or hosting platform run-time processes ID to the GRI as a provisioning session ID.
- During **Operation stage** the security services provide access control to the provisioned services and maintain the service access or usage session.
- **Decommissioning stage** ensures that all sessions are terminated, data are cleaned up and session security context is recycled. Decommissioning stage may also provide information to or initiate services usage accounting.

The proposed SSLM model extends the existing SLM frameworks and earlier proposed by authors the CRP model [5] with the additional stages “Reservation Session Binding” and “Registration & Synchronisation” which especially target such scenarios as the provisioned services/resources restoration, upgrade or migration (in the framework of the active provisioning session) and provide a mechanism for remote data protection by binding them to the session context.

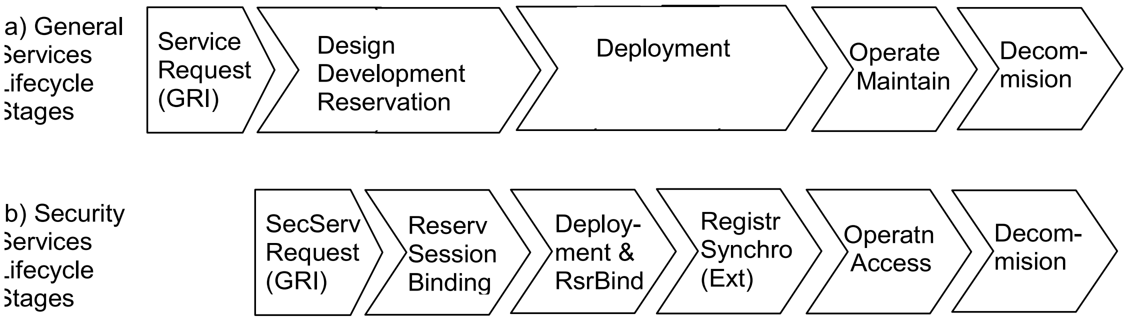

Figure 2. The proposed Security Services Lifecycle Management model.

Table 1. Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Design/Development Reservation	Deployment	Operation	Decommissioning
Process/ Activity	SLA Negotiation	Service/Resource Composition Reservation (advance)	Reservation (final) Virtualisation Configuration	Orchestration Session Management Monitoring	Logoff (global) Accounting
Mechanisms/Methods					
SLA	R				R
Workflow		(O)		R	
Metadata	R	R	R	R	
Dynamic Security Association		(O)	R	R	
AuthZ Session Context		R	(O)	R	
Logging		(O)	(O)	R	R

Legend: R – required; (O) – optional.

It is important to note that mentioned above functionality was not needed in human controlled services development and lifecycle management. It is also perceived that implementation of such functionality will require the service hosting platform that supports Trusted Computing Platform Architecture (TCPA) and corresponding technologies to support trusted virtualisation [30, 31, 32].

Table 1 explains what main processes/actions take place during the different SLM/SSLM stages and what general and security mechanisms are used:

- **SLA** used at the stage of the service Request placing and can also include SLA negotiation process.
- **Workflow** is typically used at the Operation stage as service Orchestration mechanism and can be originated from the design/reservation stage.
- **Metadata** are created and used during the whole service lifecycle and together with security services actually ensure the integrity of the SLM/SSLM.
- **Dynamic security associations** support the integrity of the provisioned resources and are bound to the security sessions.
- **Authorisation session context** supports integrity of the authorisation sessions during Reservation, Deployment and Operation stages.
- **Logging** can be actually used at each stage and especially important during the last 2 stages Operation and Decommissioning.

VI. 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 [33]. GEMBus incorporates the SOA services management paradigm in on-demand service provisioning. The Composable Services Architecture (CSA) will support different services interaction, from the infrastructure up to application elements and will provide functionality to describe, discover, access and combine services in the GÉANT environment. The GEMBus is built upon the industry accepted the Enterprise Service Bus (ESB) [34] and will extend it with the necessary functional components and design patterns 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 and orchestration under higher level application workflow. The final result will be the availability of the GEMBus Service Layer middleware for seamless access to the network based services and applications implementing the GEMBus composable services interface or adaptors.

The following functionalities 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 that 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 [35].

GEMBus design and implementation preserves the following security properties along the whole service lifecycle:

- All requests and responses exchanged through the GEMBus infrastructure must include the identity of the elements issuing it, including a unique identifier for it.
- Unique identifiers of GEMBus elements must be persistent and must not be reassigned unless the assigning authority implements necessary mechanisms to track all changes and therefore can univocally identify the corresponding element.
- Service endpoints must explicitly state their security requirements in their service description.
- To allow security service interoperability in the multi-domain environment that may use different formats of the security credentials or assertions, the GEMBus will implement a common GEMBus Security Token (GST) format. Endpoint security requirements should include their accepted statement syntaxes, and an implicit acceptance of the GST is to be considered.
- Token handling functionality can be outsourced to the separate Security Token Service (STS) that should support GST validation, federation, and mapping.

If a common token format is used or, conversely, a service able to generate appropriate tokens by translating among equivalent ones is available, there are two distinct phases in securing service access in the general case:

1) Token request and generation, that it is up to the local mechanism that the user decides to employ, as long as a minimal set of requirements on the Level of Assurance is fulfilled [36].

2) Validation of the token received by the requested service, retrieving additional attributes from the trusted sources if necessary, and requesting an access control decision from a policy decision point.

The GEMBus authentication and authorization services are integrated with the main services using aspect-oriented approach that allows easy security services integration by defining special SOAP message header fields. Additionally, GST can be used in managing inter-domain security context and authorisation sessions.

VII. 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 creates 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 analyses existing frameworks for dynamically composed services lifecycle management and proposes the Security Services Lifecycle Management model that extends the existing frameworks with the additional stages “Reservation Session Binding” and “Registration & Synchronisation” which specifically target such scenarios as the provisioned resources restoration, upgrade or migration and provide a mechanism for the remote executing environment and data protection by binding them to the provisioning session context.

The proposed SSLM is being cooperatively developed in the framework of the two EU funded projects GEANT3 and GEYSERS. Together with the general Services Delivery Framework it is considered as a major enabling component of the on-demand infrastructure services provisioning. The SSLM is currently being implemented as an architectural component of the GEANT Multidomain service bus (GEMBus). The GEMBus infrastructure is intended to allow dynamic composition of the infrastructure services to support collaboration of the distributed groups of researchers in cross-domain multi-organisational environment.

The concepts and solutions presented in this paper are considered as a potential contribution to the Open Grid Forum (OGF) Research Group on On-Demand Infrastructure Services Provisioning (ISOD-RG) which was established with the active authors’ involvement and contributions to the preceding workshops and BoF (refer to ISOD-BOF materials at OGF28 and OGF30).

The authors believe that concepts proposed in this paper will provide a good basis for further discussion among researchers about defining practical Security Services Lifecycle Management framework to build consistent security services for dynamically provisioned resources and services to support distributed collaborative infrastructures.

ACKNOWLEDGMENT

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 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] Demchenko, Y., M. Cristea, C. de Laat, E. Haleplidis, "Authorisation Infrastructure for On-Demand Grid and Network Resource Provisioning," Proceedings Third International ICST Conference on Networks for Grid Applications (GridNets 2009), Athens, Greece, 8-9 September 2009. ISBN: 978-963-9799-63-9

[6] Demchenko, Y., C. M. Cristea, de Laat, XACML Policy profile for multidomain Network Resource Provisioning and supporting Authorisation Infrastructure, IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY 2009), July 20-22, 2009, London, UK. ISBN-13: 978-0-7695-3742-9. Pp. 98-101.

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

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

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

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

[11] Willner, A., C.Barz, J.Garcia-Espin, J.F.Riera, S.Figuerola. "Harmony: Advance reservation in heterogeneous multi-domain environment." Proceedings of the 8th IFIP Networking conference, Springer's LNCS, 5 2009. ISBN: 978-3-642-01398-0

[12] Guok, C., D..Robertson, E.Chaniotakis, M.Thompson, W.Johnston, Brian Tierney, "A User Driven Dynamic Circuit Network Implementation", Proceedings DANMS2008 Conference, IEEE, July 2008.

[13] Escalona, E., G. Zervas, R. Nejabati, D. Simeonidou, G. Markidis, A. Tzanakaki, G. Carrozzo, N. Ciulli, B. Belter, A. Binczewski, "Deployment and Interoperability of the Phosphorus Grid Enabled GMPLS (G2MPLS) Control Plane," Eighth IEEE Intern. Symposium on Cluster Computing and the Grid (CCGRID), 2008. pp.716-721,

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

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

[16] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009. http://www.cloudsecurityalliance.org/csaguide.pdf

[17] Cloud Computing: Benefits, risks and recommendations for information security, Editors Daniele Catteddu, Giles Hogben, November 2009. http://www.enisa.europa.eu/ act/rm/files/deliverables/cloud-computing-risk-assessment

[18] Securing the Cloud: Designing Security for a New Age, Dec. 10, 2009. http://i.zdnet.com/whitepapers/ eflorida_ Securing_Cloud_Designing_Security_New_ Age.pdf

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

[20] GFD.80 "The Open Grid Services Architecture, Version 1.5", I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell, J. Von Reich. Open Grid Forum, September 5, 2006.

[21] Amazon Web Services: Overview of Security Processes. November 2009. http://aws.amazon.com/security

[22] 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

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

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

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

[26] TMF New Generation Operations Systems and Software (NGOSS). http://www.tmforum.org/BestPracticesStandards/ SolutionFrameworks/1911/Home.html

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

[28] NIST Special Publication 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology. September 1996. http://csrc.nist.gov/ publications/nistpubs/800-27/sp800-27.pdf

[29] Microsoft Security Development Lifecycle, Version 5.0, March 31, 2010. http://www.microsoft.com/sdl

[30] TCG Infrastructure Working Group Reference Architecture for Interoperability. Specification Ver. 1.0. 16 Jun. 2005. http://www.trustedcomputinggroup.org/ specs/IWG/IWG_Architecture_v1_0_r1.pdf

[31] Demchenko Y., Frank Siebenlist, Leon Gommans, Cees de Laat, David Groep, Oscar Koeroo, "Security and Dynamics in Customer Controlled Virtual Workspace Organisation," Proc. HPDC2007 Conference, Monterey Bay California, June 27-29, 2007.

[32] Löhr, H., H.V.Ramasamy, A.Sadeghi, S.Schulz, M.Schunter, C.Stüble, "Enhancing Grid Security Using Trusted Virtualization, in Autonomic and Trusted Computing," Lecture Notes in Computer Science, 2007, Volume 4610/2007, 372-384, DOI: 10.1007/978-3-540-73547-2_39

[33] 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

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

[35] 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.

[36] NIST SP 800-63 Electronic Authentication Guidance - NIST Special Publication 800-63, Version 1.0.2. [Online] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf