Services lifecycle management in on-demand services/resources provisioning

ITU-T, OASIS and other industry standards overview

WP3 Technical document, Version 0.1

Yuri Demchenko, UvA

1 Introduction

This document provides information about existing standards and technologies related to the definition of the provisioned on-demand resources and services that should provide a basis for the development of the Geysers architecture and implementation of its components.

One of the intended goals of this work is to illustrate that development of the consistent security services will require first and will rely on the precise definition of the general services architecture.

2 Standard Frameworks Related to On-Demand Services and Resources Provisioning

2.1 NGN Open Service Environment (OSE)

Recent ITU-T and TMF standards and projects related to the definition of the Next Generation Network (NGN) and so-called NGN Open Service Environment (OSE) concept demonstrate present trend to using Service-Oriented Architecture (SOA) concepts [1] in modern telecommunication industry [2]. Reviewing corresponding ITU-T standards can provide useful information for designing a consistent and sustainable Geysers architecture and its functional components and services.

It is a natural step that NGN technology are moving to adopting SOA concepts and Web Services based services integration model to build Open Service Environment (OSE) as pre-scribed by another set of ITU-T standards defining NGN convergence model based on Web Services [6] and required NGN capabilities to support OSE [7]. Web services enabled NGN transport networks provide a native environment for integrating applications, services and resources that can be provisioned on-demand.

The Next Generation Networks (NGN) is introduced by ITU-T as a next step in creating Global Information infrastructure. The NGN principles and the general reference model specified in the ITU-T Recommendation Y.2011 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.

A number of the recent ITU-T recommendations related to the Next Generation Network (NGN) provide a basis for transport/network and Information Technology (IT) convergence based on NGN. The NGN reference model, according to ITU-T Y.2011 Recommendation [3], suggests separation of the transport network and application services and defines them as NGN service stratum and NGN transport stratum consisting of User plane, Control plane and Management plane. The ITU-T Recommendations Y.2012 and Y.2201 specify high level requirements and functional architecture of the NGN Release 1 [4, 5]. The described NGN service architecture implements services and network separation principle and defines functional components of the Transport stratum and Service stratum. The NGN Y.2012 architecture defines also Application Network Interface (ANI) that provides an abstraction of the network capabilities and is used as a channel for applications to access network services and resources.

The NGN convergence service model is defined by ITU-T Recommendation Y.2232 and suggests the major scenario with using Web Services [6]. The NGN Open Service Environment (OSE) defined by ITU-T Recommendation Y.2234 [7] is based on Web Services and actually implements basic SOA principles in defining a services integration model. The definition of the OSE and Web Services convergence model is targeted to provide common framework for both applications developers and provider services developers.

The Y.2234/Y.2201 NGN OSE is required to satisfy such requirements as independence from transport network providers, independence from manufactures, location transparency, network transparency, and protocol transparency. The OSE should provide the following capabilities to support effective services integration and operation: service coordination; interworking with service creation environment; service discovery; service registration; policy enforcement; and development support. The latter capability actually suggests that OSE should “support the full lifecycle of components, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal.

2.2 Compliance with the standard SOA frameworks

It is suggested that Geysers architecture should based on and should support the basic SOA architectural principles and services interaction models [1, 8].

As correctly noted in [9] “SOA is based on business requirements” and “aligns IT and business so that IT systems work the way the business does, helping to ensure that IT produce business value”. From the service design point of view this means that SOA based services and the services design and deployment process should allow and use different levels of abstraction and ensure the whole services delivery lifecycle.

In its evolution and gradual development Geysers services architecture should adopt SOA best practices and comply with the Open Group Services Integration Maturity Model (OSIMM) [10]. The OSIMM defines a grid of the 7 maturity level and 7 dimensions that describe provisioned services and SOA related properties. The 7 OSIMM maturity levels include:

(OSIMM1) Silo;

(OSIMM 2) Integrated;

(OSIMM 3) Componentised;

(OSIMM 4) Services,

(OSIMM 5) Composable services;

(OSIMM 6) Virtualised services;

(OSIMM 7) Dynamically re-configurable services.

The 7 dimensions define different presentation layers and aspects of the services such as Business view, Governance and Operations, Methods, Applications, Architecture, Information, Infrastructure and Management.

In Applications dimension the SOA based applications deal with the different the components and building blocks mapped to the above defined maturity levels: modules (OSIMM1), objects (OSIMM2), components (OSIMM3), services (OSIMM4), applications comprised of services (OSIMM5), process integration via services (OSIMM6), and dynamic application assembly (OSIMM7). Starting from the level "OSIMM4 - Services" the information or data are represented as Information as a service (OSIMM4), Data dictionary and repository (OSIMM5), Virtualised data services (OSIMM6), Semantic data vocabularies, correspondingly (OSIMM7). Table 1 provides summary of the services presentation models at the different OSIMM levels.

The OSIMM also defines so-called domains that are specific problem areas projected into the Maturity – Dimensions grid. Starting from the "Level 4 – Services" the security services are considered as a basic service that according to the OSIMM model can be composed, virtualised and dynamically reconfigured. This implies more requirements to defining the GMI discussed in this document.

Table 1. SOA components presentation at different OSIMM levels.

OSIMM levels & Dimensions	OSIMM1 Silo	OSIMM2 Integrated	OSIMM3 Componentised	OSIMM4 Services	OSIMM5 Composable services	OSIMM6 Virtualised services	OSIMM7 Dynamically re-configurable services
Business view	Isolated business lines	Business process integration	Componentised business	Componentised business offers services	Processes through services composition	Geographical independent service centers	Mixed match business and context aware-capabilities
Organisation	Ad hoc IT strategy & Governance	Ad hoc enterprise strategy & Governance	Common Governance process	Enabling SOA Governance	SOA and IT Governance Alignment	SOA and IT Infrastructure Governance Alignment	Governance through policy
Methods	Structured analysis and Design	Object Oriented Modeling	Component based development	Service Oriented Modeling	Service Oriented Modeling	Service Oriented Modeling for Infrastructure	Business Grammar Oriented Modeling
Applications	Modules	objects	components	services	applications comprised of services	process integration via services	dynamic assembly, context-aware invocation
Architecture	Monolithic architecture	Layered architecture	Component architecture	Emerging SOA	SOA	Grid based SOA	Dynamically re-configurable architecture
Information	Application specific	LOB or enterprise specific	Canonical models	Information as a service	Enterprise Business Data dictionary and repository	Virtualised data services	Semantic data vocabularies
Infrastructure (and Management)	LOB Platform specific	Enterprise standards	Common re-usable infrastructure	Project based SOA environment	Common SOA environment	Virtual SOA environment, S&R	Dynamic sense, Decide& Responde
	OSIMM1	OSIMM2	OSIMM3	OSIMM4	OSIMM5	OSIMM6	OSIMM7

2.3 Composable Services Lifecycle Management

The SOA based technologies provide a good basis for creating composable services which in case of advancing to dynamically re-configurable services should also rely on the well-defined services lifecycle management (SLM). Most of existing SLM frameworks and definitions are oriented on rather traditional human-driven services development and composition. 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.

Figure 1 (a) illustrates typical sequence of stages defining the provisioned service lifecycle that includes service request, design or development, deployment or implementation, operation, retire or disposal. These stages are quite in tact with the proposed [11] Complex Resource Provisioned (CRP) model which was proposed for on-demand Network resources provisioning in Phosphorus project [12].

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. However, 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 of the service context management together with ensuring integrity of the security context itself. The problem here is that such mechanisms are generically stateful what impose problems for SOA environment which is defined as generically stateless.

The NIST Special Publication 800-14 “Generally Accepted Principles and Practices in Systems Security” [13] together with SP 800-27 “Engineering Principles for Information Technology Security” [14] define a basic set of the generally accepted principles and practices for designing and managing security services. The defined security services lifecycle includes the following phases: Initiation, Development/Acquisition, Implementation, Operation/Maintenance, and Disposal. Providing a good basis for security services management, these principles still reflect the traditional approach to services and systems design driven by engineers force.

To answer dynamic character of the New Generation Networks (NGN) concept [5, 6], the TeleManagement Forum (TMF) [15] proposed the Service Delivery Framework (SDF) [16] as a part of their New Generation Operations Systems and Software (NGOSS) solutions framework [17]. The main motivation behind developing SDF is achieving automation of the whole service delivery and operation process. The SDF principles include:

- End-to-end service management in a multi-service providers environment
- End-to-end service management in a composite, hosted and/or syndicated service environment

Management functions to support a highly distributed service environment, for example, unified or federated security, user profile management, charging etc.

The SDF defines two basic supporting systems: Management Support Service (SDF MSS) and Infrastructure Support Service (ISS), that support the main SDF stages design, deployment, and operation,

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” [13], 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/Acquisition, Implementation, Operation/Maintenance, and Disposal.

Figure 1 (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 and/or infrastructure. The SSLM includes the following stages:

- Service request and generation of the GRI that will serve as a provisioning session identifier and will bind all other stages and related security context.
- Reservation session binding that provides support for complex reservation process 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 Global Reservation ID (GRI) as a common provisioning session ID.
- Registration&Synchronisation stage (that however can be considered as optional) that specifically targets possible scenarios with the provisioned services migration or failover. 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.
- 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.

The proposed SSLM model extends the existing SLM frameworks and earlier proposed by authors the CRP model [13] with the new stage “Registration & Synchronisation” that specifically targets such security issues as the provisioned services/resources restoration (in the framework of the active provisioning session) and provide a mechanism for remote data protection by binding them to the session context. However, it is perceived that implementing such functionality will require the service hosting platform that supports Trusted Computing Platform Architecture (TCPA) [27, 28].

Table (c) in Figure 1 also 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 essentially important during the last 2 stages – Operation and Decommissioning.

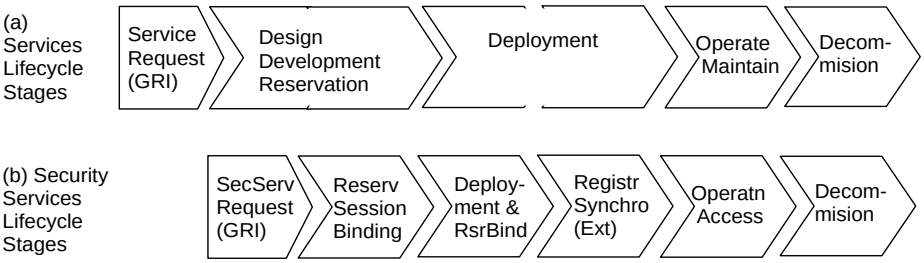

Table (c). Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Design/Reservation Development	Deployment	Operation	Decomissioning
Process/ Activity	SLA Negotiation	Service/ Resource Composition Reservation	Composition Configuration	Orchestration/ Session Management	Logoff Accounting
Mechanisms/Methods					
SLA	**V**				**V**
Workflow		(V)		**V**	
Metadata	**V**	**V**	**V**	**V**	
Dynamic Security Associatn		(V)	**V**	**V**	
AuthZ Session Context		**V**	(V)	**V**	
Logging		(V)	(V)	**V**	**V**

Figure 1. The proposed Security Services Lifecycle Management model.

3 Security Issues in Cloud Computing as Infrastructure Services

Most of Grid/Cloud usage scenarios for collaboration can benefit from combined Grid and network resource 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 and network-resource provisioning requires that a number of services and resource controlling systems should 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 can not 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 probably they will evolve into general IT resources, providing a basis for true New Generation Networks (NGN). 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 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.

The current Cloud services implement three basic provisioning models: utility computing, Platform as a Service (PaaS), and Software as a Service (SaaS) [18]. 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 Cloud security that finally demonstrate convergence of the proposed security models for Clouds and provide detailed analysis of the Clouds operation [19, 20, 21].

The major difference comparing to Grids is that in Clouds data are processed in the environment that is not under the direct user or data owner control. This control can potentially be compromised by either Cloud insiders or by other users. Data/information must be secured during all processing stages – upload, process, store, stream/visualize. Policy and security requirements must be bound to the data themselves and there should be necessary security mechanisms in place to enforce these policies.

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

- Secure data transfer that should be enforced with 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 are based on the 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 NGN will require implementing security mechanisms for the remote control of the Cloud operational environment integrity by users. Current practice by Clouds providers is mostly based on SLA that describes also security measures taken by the provider but don't define mechanisms for checking them by users, like in case of Amazon Web Services (AWS) Cloud service [20].

4 References

1. 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
2. ITU-T Recommendation Y.2001 (2004) - General overview of Next Generation Networks (NGN). http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2001-200412-I!!PDF-E&type=items

3. ITU-T Recommendation Y.2011 (2004) - General principles and general reference model for Next Generation Networks.

4. ITU-T Recommendation Y.2012 (09/2006) - Functional requirements and architecture of the NGN release 1.

5. ITU-T Recommendation Y.2201 (04/2007) - NGN release 1 requirements .

6. ITU-T Recommendation Y.2232 (01/2008) - NGN convergence service model and scenario using web services .

7. ITU-T Recommendation Y.2234 (09/2008) - Open service environment capabilities for NGN

8. IBM's SOA Foundation: An architectural introduction and overview. Whitepaper. November 2005. http://download.boulder.ibm.com/ibmdl/pub/software/dw/webservices/ws-soa-whitepaper.pdf

9. ESB-oriented architecture: The wrong approach to adopting SOA, by Bobby Woolf, WebSphere SOA and J2EE Consultant, IBM. http://www.ibm.com/developerworks/webservices/library/ws-soa-esbarch/

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

11. 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

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

13. 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

14. NIST Special Publication 800-27 - Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001. National Institute of Standards and Technology. - http://csrc.nist.gov/ publications/nistpubs/800-27/sp800-27.pdf

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

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

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

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. 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

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

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

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

23. Web Services Security Roadmap (2002). [Online]. Available: http://www.ibm.com/developerworks/library/ specification/ws-secmap/

24. 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, Sept. 5, 2006.

25. WS-I Basic Profile Version 1.1 (2006), WS-I Basic Profile Version 1.1. <http://www.ws-i.org/Profiles/BasicProfile-1.1.html>

26. WS-I Basic Security Profile Version 1.0 (2007), Basic SecurityProfile Version 1.0. <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

27. 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.

28. Trusted Computing Group (TCG). [Online]. Available: https://www.trustedcomputinggroup.org/home