Service Delivery Framework and Services Lifecycle Management in on-demand services/resources provisioning

WP2/WP3 Technical document, Version 0.2

Editor:
Yuri Demchenko, UvA

Contributors:
Yuri Demchenko, UvA
Xiaomin Chen, TUBS

1 Introduction

This document provides overview of the existing service delivery and lifecycle management frameworks and presents the proposed Service Delivery Framework (SDF) for on-demand infrastructure services provisioning information being developed in the framework of the GEYSERS Project.

The document provides also suggestions about development of the consistent security services that can be provisioned dynamically together with on-demand infrastructure services provisioning that relies on the general SDF.

2 Existing Service Lifecycle Management Frameworks

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) [1, 2]. 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 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 [3] Complex Resource Provisioned (CRP) model which was proposed for on-demand Network Resources Provisioning in the Phosphorus project [4].

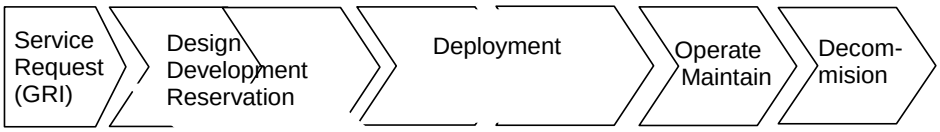

Figure 1. General Services Lifecycle Management model

To answer dynamic character of the New Generation Networks (NGN) concept, the TeleManagement Forum (TMF) [5] proposed the Service Delivery Framework (SDF) [6] as a part of their New Generation Operations Systems and Software (NGOSS) solutions framework [7]. The main motivation behind developing SDF is achieving automation of the whole service delivery and operation process, in particular:

- 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.
- Any other scenario that pertains to a given phase of the service lifecycle challenges, such as on boarding, provisioning, or service creation.

SDF services lifecycle corresponds to the general services lifecycle management model shown on Figure 1. Figure 2 illustrates the major SDF components and their interactions during 3 main stages Design, Deployment, Operation. The SDF defines two basic supporting systems: Management Support Service (SDF MSS) and Infrastructure Support Service (SDF ISS). The Service instance, delivered or provisioned on demand, is presented as containing: (2) Service Management Interface, (3) Service Functional Interface, and (3a) Service Consumer Interface.

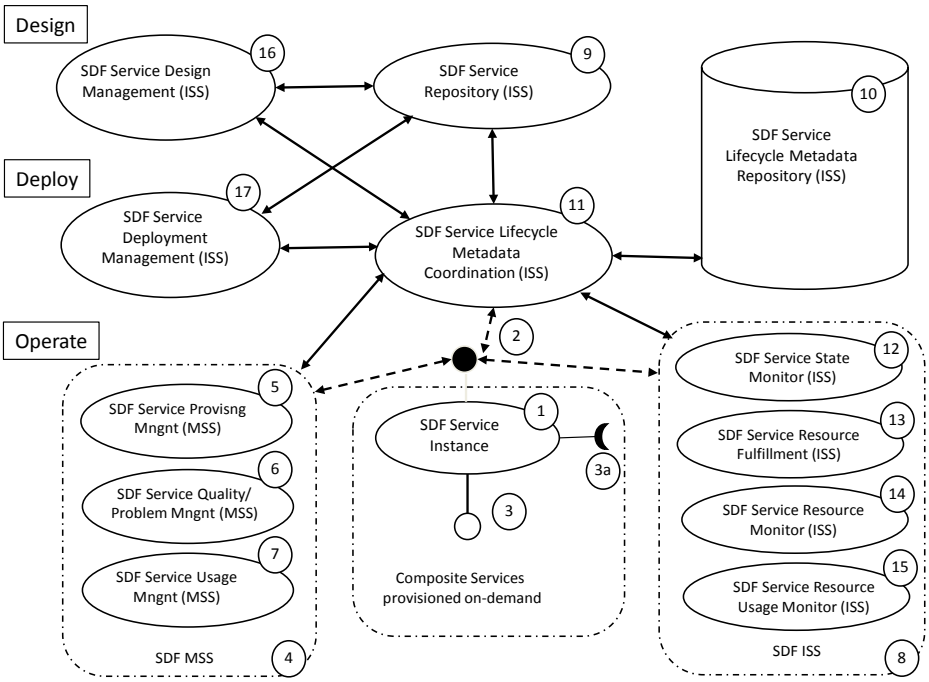

Figure 2. SDF main components and their interaction during Design, Deployment and Operation Stages

The framework specifies the following components involved into the service provisioning at different lifecycle stages:

SDF Stages				
REQUEST	DESIGN stage	DEPLOYMENT stage	OPERATION stage	DECOMMISSION
SLA Negotiation	9 - Service Repository	10 - Service Lifecycle Metadata Repository	5 - Service Provisioning Management	10 - Service Lifecycle Metadata Repository
Provisioning Session ID assignment	10 - Service Lifecycle Metadata Repository	11 - Service Lifecycle Metadata Coordinator	6 - Service Quality/Problem Management	11 - Service Lifecycle Metadata Coordinator
11 - Service Lifecycle Metadata Coordinator	16 - Service Design Management	17 - Service Deployment Management	7 - Service Usage Monitor	14 - Service Resource Monitor
			11 - Service Lifecycle Metadata Coordinator	15 - Resource Usage Monitor
			12 - Service State Monitor	

			13 - Service Resource Fulfillment	
			14 - Service Resource Monitor	
			15 - Resource Usage Monitor	

It is important to mention that the key component of the SDF model is Services/resource Lifecycle Metadata management. This system and a process is designated to ensure the consistency of the service management and in particular important to support consistent security services provisioning and management.

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” [8] together with SP 800-27 “Engineering Principles for Information Technology Security” [9] 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.

3 GEYSERS Services Delivery Framework

GEYSERS Service Delivery Framework defines a basic virtual infrastructure (VI) provisioning workflow and its operation during on-demand infrastructure services provisioning [10]. It can be considered as TMF SDF profile/implementation for the specific use case of on-demand infrastructure services provisioning.

Note. Currently this section uses GEYSERS terminology, however it is suggested that with wider adoption of the proposed framework the terminology will evolve to more generic.

3.1 General Virtual Infrastructure provisioning workflow

The GEYSERS Service Delivery Framework (SDF) supports two types of services, namely, Virtual Infrastructure (VI) provisioning and on-demand infrastructure services provisioning. The first service aims to create a VI on the request from the Virtual Infrastructure Operator (VIO), two other actor participating in this process are Physical Infrastructure Provider (PIP) and Virtual Infrastructure Provider (VIP) defined in the GEYSERS project. The on-demand infrastructure services provisioning is done on the request from the user or application on behalf of user for the specific task or project.

The workflow of the VI provisioning is shown in Figure 3, which comprises five phases, namely, (1) Service requests and SLA negotiation; (2) Planning/design; (3) Deployment/Configuration; (4) Operation and (5) Decommission. The on-demand service provisioning is the major activity in the operation phase of virtual infrastructure provisioning, which also consists of five phases as shown in Figure 3. The GEYSERS SDF

intends to be compliant with the TMF Service Delivery Framework [6] discussed above above with the necessary extensions to facilitate the combined network + IT services.

The GEYSERS SDF is designed to support the novel business and operational models, including the automated and manual provisioning of the virtual infrastructure, defined as automated VI provisioning and VIO-triggered VI provisioning. Both cases rely on the pre-condition that one or more PIPs expose their owned physical resources to enable its virtualization and subsequent leasing. The VIPs can compose their virtual infrastructure by selecting the virtual resources from the virtual resource pool. The automated VI provisioning composes the required VI by running dynamic online algorithms and configures the network and IT resource controllers (i.e., Network Control Plane (NCP), and VI and IT resources Manager (VITM) that also may referred to as Service Middleware Layer (SML)) automatically for the composed VI. However, manual composition of the VI can also be required. In the VIO-triggered VI provisioning scenario, the VIP has to compose the required VI by manually selecting virtual resources and negotiating with the related PIPs. Despite of the different working modes of the VI provisioning, a generic workflow framework can be applied to both cases as shown in Figure 3.

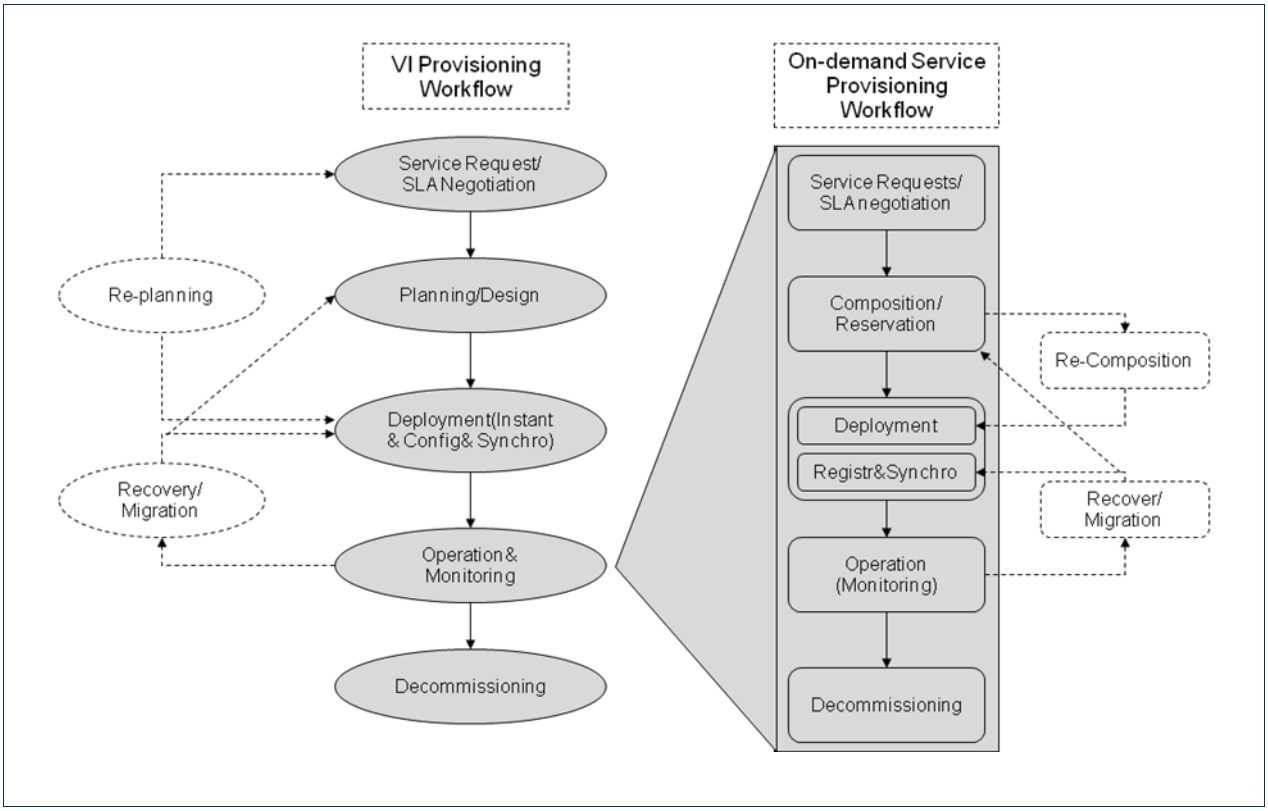

Figure 3: The generic workflow chart of the GEYSERS SDF

The on-demand service provisioning workflow is an inner cycle in the operation phase of the overall virtual infrastructure provisioning, as shown in Figure 2. In contrast to the VI provisioning which is provided for a carrier grade customer, the on-demand service provisioning is designated to provide IT + Network services for specific applications, projects or missions. It should be noted that the on-demand service provisioning requires that the VI is already created and all specified GEYSERS infrastructure interfaces are ready.

3.2 VI Provisioning

The GEYSERS VI Provisioning includes both automated and engineer/human assisted procedures. However, it is a practical requirement that all stages and the whole planned/designed infrastructure can be reviewed and re-iterated by the PIPs or VIPs. There should also be a possibility to include both legacy resources and ordinary Internet links if required resources cannot be provided by the resources supporting GEYSERS virtualization.

3.2.1 Service Request/SLA Negotiation

In this phase, the VIO defines the requirements for the desired virtual infrastructure and initiates the SLA negotiation with VIP. The Service Level Agreement (SLA) defined in this phase will provide a set of basic requirements, which can include the QoS requirements, security policies, robustness requirements etc. The security policies defined in this phase will be used in the planning, deployment and operation phases. Additionally, SLA may also contain trust anchors in a form of public key certificates. It is an initiation point of the virtual infrastructure lifecycle.

3.2.2 Planning/Design Phase

The virtual infrastructure planning can be decoupled into the following sub-phases:

- **Virtual Infrastructure design:** The Virtual Infrastructure design is carried out by a VIP based on the requirements received from the service requests and SLA negotiation phase. These requirements are in form of SLAs that are expected to be fulfilled for the service provisioning. These SLAs are decomposed into more technical constraints in the SML in a semi-automated fashion. The SML is a rule-based expert system which can also support a human interaction for planning. Fully automated planning schemes are also considered in GEYSERS SML.
- **Virtual resources selection and composition:** In this sub-phase, the VIP searches/negotiates the virtual resources from physical infrastructure layer. The resources can be composed from multiple PIPs. Algorithms are run for composition of IT and network resources. As a result, a blueprint of the virtual network is available, and ready to be included in a contract between the VIO and the VIP.
- **Virtual resource reservation:** In this sub-phase, each selected resource is associated with a common reservation ID (to be hereafter referred to as Global Reservation ID (GRI)) that also binds the reservation session/instance with the SLA initiated the provisioning process. The reserved resources need to be configured and initiated in the deployment phase.

3.2.3 Deployment Phase

During virtual infrastructure deployment phase, the reserved infrastructure instances are instantiated, configured, registered, and initialised. This phase should allow network/IT engineer review and approval. The deployment phase can be decoupled into the following sub-phases:

- **NCP and VITM instantiation and deployment**: in this sub-phase, the VIO deploys its NCP by taking consideration of the virtual infrastructure specifications. The software modules are then

deployed/installed to control the virtual network nodes. Similarly the VITMs related to the IT virtual resources are deployed/installed.

- **Configuration of NCP and VITM controllers:** The network controllers and PCE modules deployed in NCP are configured with network topology information, policies, etc. Similarly the VITM controllers are configured with information about virtual IT resource availability and properties.
- **NCP initialization:** The NCP modules are initialized and started. The network auto-configuration process takes place: e.g. neighbour/UNI discovery, initial flooding of TE parameters, routing protocol convergence, etc. In this phase the VITM also injects the capabilities of the IT site under its control into the NCP.
- **Instant Network+IT service/infrastructure registration and initialisation**: this sub-phase allows a new service registered in VIO and put into operation. It also allows binding security and provisioning session with the service ID and (underlying/implementing) platform runtime environment. Importance of specifying this phase is defined by the need to address such scenarios as infrastructure re-planning and failure restoration.

As a result of the instantiation phase, the VIO has configured the virtual resources and has deployed its control plane for the virtual infrastructure. The virtual infrastructure is up and running.

3.2.4 Operation phase

The operation phase includes all the processes for provisioning of network + IT services (NIPS) to users. During the operation phase the VIO runs its own virtual infrastructure provisioning service that targeted to deliver necessary infrastructure resources (both network and IT) to users, project or applications. It is intended that this provisioning process is maximum automated and allows using the same business model as traditional physical operators. The on-demand service provisioning happens in this phase, which will be elaborated in the next section.

3.2.5 Re-planning and Recovery Phases

Re-planning and recovery phases are additional phases triggered by special events during operation or on the request of any of actors. Re-planning is a special virtual infrastructure stage in which the virtual infrastructure virtualisation and management service implements changes to the virtual infrastructure. It can be triggered at any time once the virtual infrastructure has been instantiated. The VIO can ask the VIP for re-planning if it is interested in upgrades to the a priori negotiated virtual resources or the VIP itself can trigger the re-planning procedures for optimization and recovery purposes. The potential triggers for the re-planning process can be summarized as follows.

- NCP (Network Control Plane, only for the network side): The NCP could request a virtual infrastructure re-dimensioning based on medium- and long-term resource availability, and taking into account VIP-N/VIO-N SLAs for variations in virtual resource provisioning.
- SML (Service Middleware Layer): The SML could trigger a similar process regarding the IT resources availability.
- Failure driven: A failure in a virtual element forces the LICL to search for an alternative resource (in an automated way).
- LICL (Logical Infrastructure Composition Layer): LICL maintenance may require the migration of the virtual infrastructure components to another physical resource, what should be done in a seamless way.

As the main effect of re-planning is upgrade of the virtual infrastructure, the new infrastructure layout have be (re-)deployed and NCP and VITM have to be re-configured. It is important that infrastructure re-planning or upgrade can be done incrementally and in a such way that the current virtual infrastructure operation is not affected. Re-planning can be governed by policies stated in the SLAs negotiated during the original planning phase or may require negotiation of new SLAs between VIO and VIP as well as VIP and PIP.

Restoration phase/process takes place when running virtual/provisioned service fails, e.g. because of hardware failure. Depending on type of failure, restoration may require just re-starting/re-deploying virtual service or will involved planning/design/reservation processes.

3.2.6 Decommissioning Phase

Decommissioning phase is triggered whenever a Virtual Infrastructure is no longer in operation and must be decommissioned. This usually happens when the leasing contract between VIP and VIO ends and the virtual infrastructure is no more suitable for other VIO customers of the VIP. The termination phase comprises all the processes to properly decommissioning the physical resources of the virtual infrastructure. It ensures that all the authorization right of the VIP for access to the PIP resources are inactivated as well as the authorization right of the VIO for access to the virtualized physical resources. Once a virtual infrastructure is decommissioned, the physical resources of the PIPs become available for planning and instantiation of new virtual infrastructures.

3.3 On-demand Infrastructure services provisioning workflow

Figure 3 (which is the re-drawn right part of Figure 2) illustrates the main on-demand service provisioning or delivery stages:

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

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

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

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

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

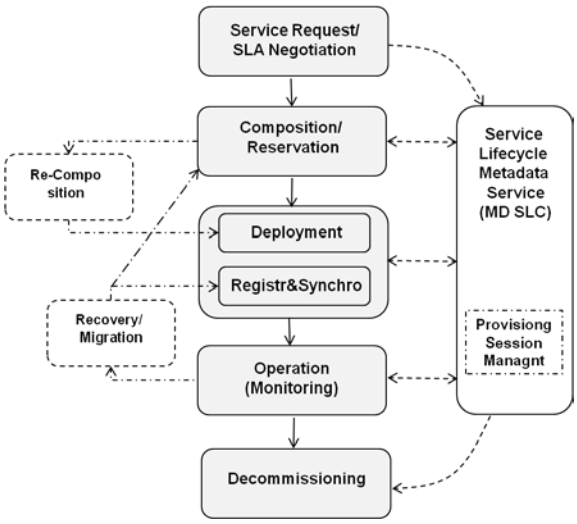

Figure 3. On-demand Infrastructure (Composable) Services Provisioning Workflow.

The two additional (sub-)stages can be initiated from the Operation stage and/or based on the running composed service or component services state, such as their availability or failure:

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

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

3.4 Infrastructure services to support SDF

Implementation of the proposed SDF requires a number of special Infrastructure Support Services (ISS) to support consistent (on-demand) provisioned services lifecycle management (similar to mentioned above TMF SDF [6] and Fig. 2) that can be implemented as a part of the virtual infrastructure management middleware (VIM MW).

The following services are essential to support consistent Service Lifecycle Management:

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

4 SDF and Consistent Security Services Provisioning

4.1 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 [11, 12], and probably they will evolve into general IT resources, providing a basis for true New Generation Networks (NGN) [13, 14]. 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) [12]. 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 demonstrated convergence of the proposed security models for Clouds and provide detailed analysis of the Clouds operation [15, 16, 17, 18].

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 [17].

4.2 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" [8], 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 4 (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 (SessionID) and will bind all other stages and related security context. The Request stage may also include SLA negotiation which will become a part of the binding agreement to start on-demand service provisioning.
- **Reservation stage** and 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 [3] 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.

Table (c) in Figure 4 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.

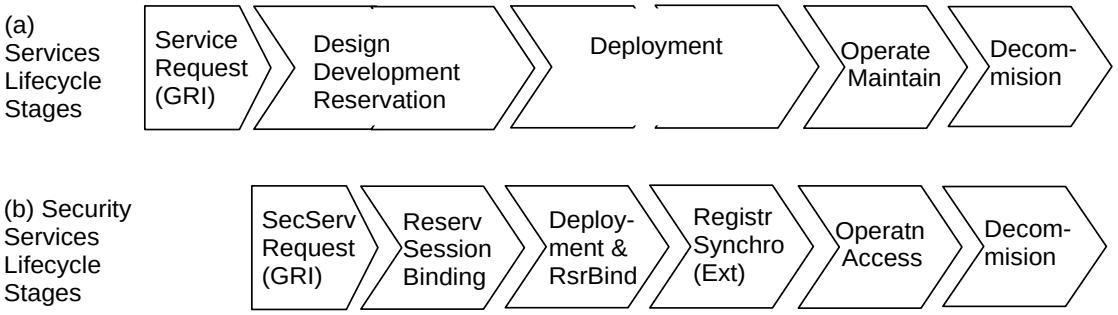

Table (c). Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Design/Reserv. 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**	
Service Lifecycle Metadata	**V**	**V**	**V**	**V**	
Dynamic Security Associatn		(V)	**V**	**V**	
AuthZ Session Context		**V**	(V)	**V**	

Logging		(V)	(V)	**V**	**V**

Figure 4. The proposed Security Services Lifecycle Management model.

5 Suggestions for Future Development

To be provided.

Appendix A. Open Group Service Integration Maturity Model (OSIMM)

In its evolution and gradual development the GEMBus should adopt SOA best practices and comply with the Open Group Services Integration Maturity Model (OSIMM) [2], The OSIMM defines a grid of the 7 maturity level and 7 dimensions that describes provisioned services. The 7 OSIMM maturity levels include:

(1) Silo;
(2) Integrated;
(3) Componentised;
(4) Services,
(5) Composable services;
(6) Virtualised services;
(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 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 CSA discussed in this document.

Table A1. SOA components presentation at different OSIMM levels

OSIMM levels & Dimensions	OSIMM1 Silo	OSIMM2 Integrated	OSIMM3 Componentized	OSIMM4 Services	OSIMM5 Composable services	OSIMM6 Virtualised services	OSIMM7 Dynamically re-configurable services
Business view	Isolated business lines	Business process integration	Componentized business	Componentized 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& Respond
	OSIMM1	OSIMM2	OSIMM3	OSIMM4	OSIMM5	OSIMM6	OSIMM7

6 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. The Open Group Service Integration Maturity Model (OSIMM). https://www.opengroup.org/projects/osimm/ uploads/40/17990/OSIMM_v0.3a.pdf
3. 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
4. Phosphorus Project. [Online]. Available: http://www.ist-phosphorus.eu/
5. TeleManagement Forum. http://www.tmforum.org/
6. TMF Service Delivery Framework. http://www.tmforum.org /servicedeliveryframework/4664/home.html
7. TMF New Generation Operations Systems and Software (NGOSS). http://www.tmforum.org/BestPracticesStandards/ SolutionFrameworks/1911/Home.html
8. 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
9. 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
10. GEYSERS Deliverable D2.1 “Initial GEYSERS Architecture and Interfaces Specification”
11. 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
12. NIST Definition of Cloud Computing v15. [Online] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
13. ITU-T Recommendation Y.2011 (2004) - General principles and general reference model for Next Generation Networks.

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

15. 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

16. 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

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

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