Security Services Lifecycle Management and GEYSERS Service Delivery Framework

Yuri Demchenko, UvA

Cloud Security BOF

26 October 2010

OGF30 25-28 October 2010, Brussels

Outline

- Cloud Security – New challenges
- On-Demand Infrastructure Services Provisioning
- Background – TMF Service Delivery Framework (SDF)
- GEYSERS SDF
- Security Services Lifecycle Management

Cloud Security – New challenges

Clouds as infrastructure services provisioning model/environment

- Security along the whole provisioning process and service/infrastructure lifecycle
- Manageable/user controlled security
- Securing remote executing environment
- Security context/session management

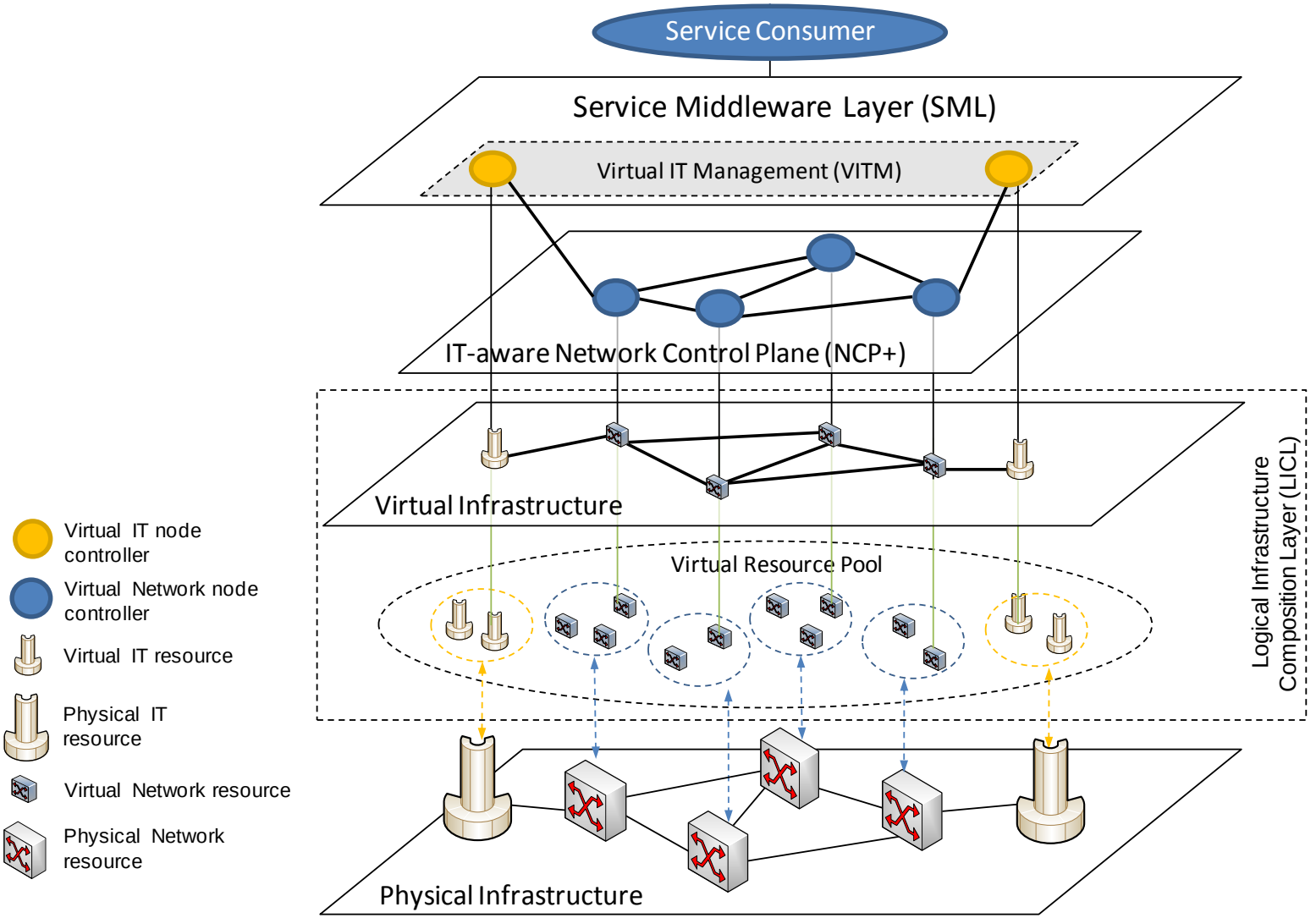
Security Service Lifecycle Management in On-Demand Resources/Services Provisioning

- On-Demand Infrastructure Services Provisioning requires definition of Services Lifecycle Management
  - Multidomain multi-provider environment
  - Includes standard virtualisation procedures and mechanisms
- Requires dynamic creation of Security/Trust Federations in multi-domain environment
- Access control infrastructure dynamically created and policy/attributes dynamically configured
  - Access/authorisation session/context management

GEYSERS Service Delivery Framework (SDF)

- Service provisioning workflow by VIP:
  - Creation of the Virtual Infrastructure (VI)
  - May include more engineers support
- Service provisioning workflow by VIO:
  - Creation and operation of the Virtual Infrastructure on-demand for specific project, tasks or user groups
  - Should be completely automatic
- Should also include activities/stages for infrastructure re-planning, restoration and migration
- Adopted TeleManagement Forum Service Delivery Framework (TMF SDF)
- GEYSERS Project - http://www.geysers.eu/

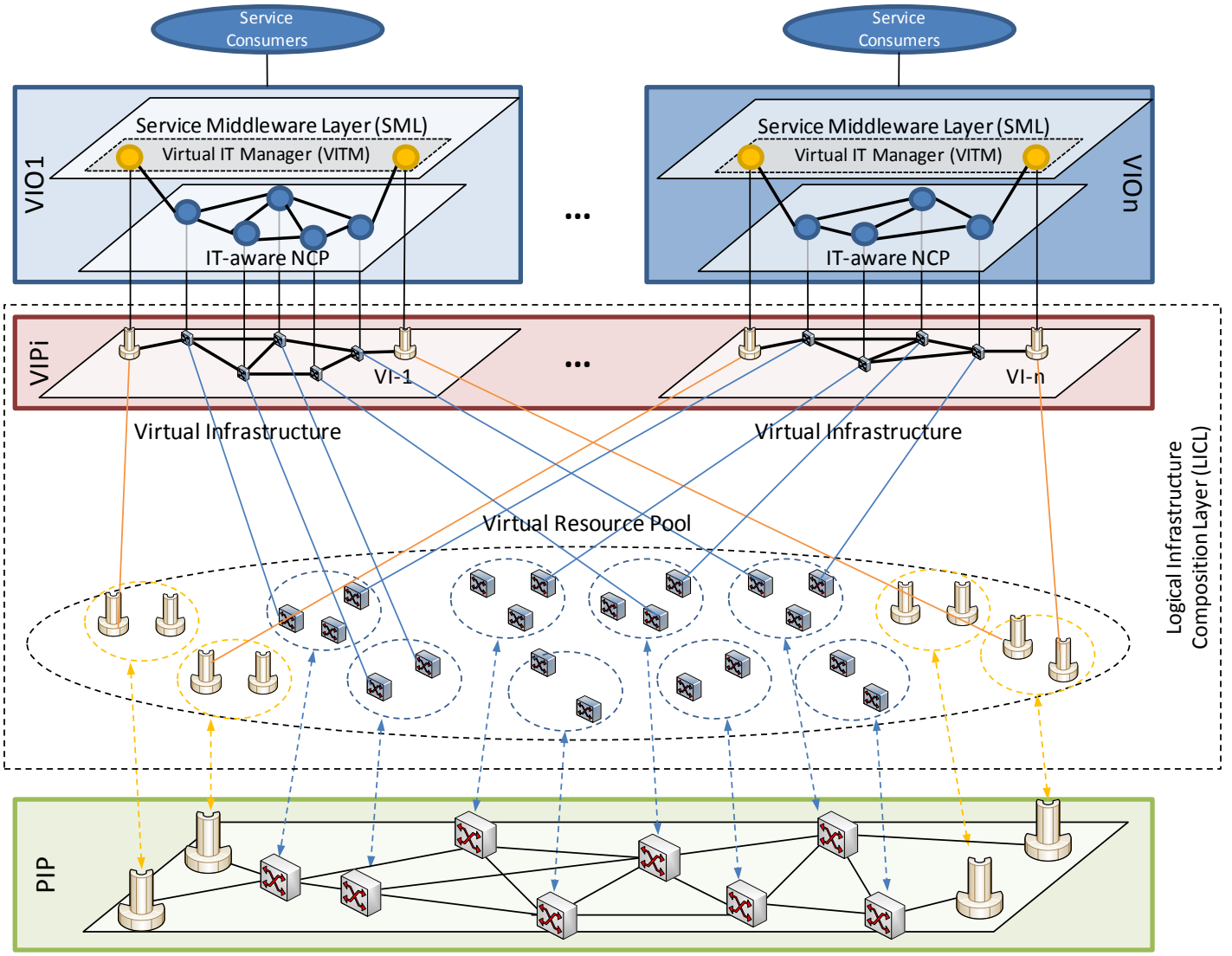
GEYSERS Reference Model



Role:

- VIO
- VIP
- PIP

Role of GEYSERS actors with respect to its architectural layers

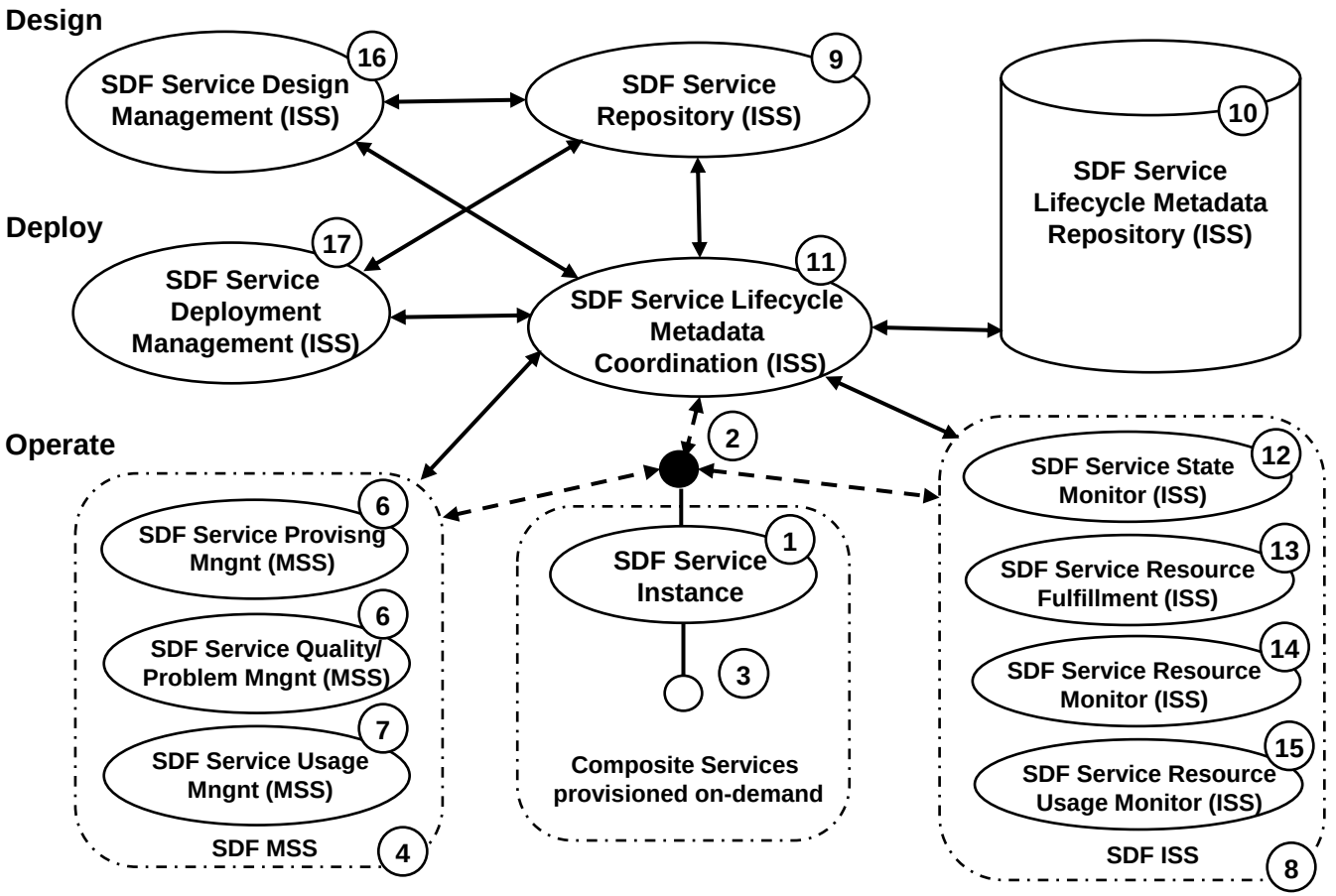


TMF Service Delivery Framework (SDF)

Goal: Automation of the whole service delivery and operation process (TMF SDF, http://www.tmforum.org/ServiceDeliveryFramework/4664/home.html)

- 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 Reference Architecture (refactored from SDF)



1 – Service Instance
2 - Service Management Interface
3 – Service Functional Interface
4 - Management Support Service (SDF MSS)
8 - Infrastructure Support Service (ISS)

DESIGN stage

9 - Service Repository
10 - Service Lifecycle Metadata Repository
16 - Service Design Management

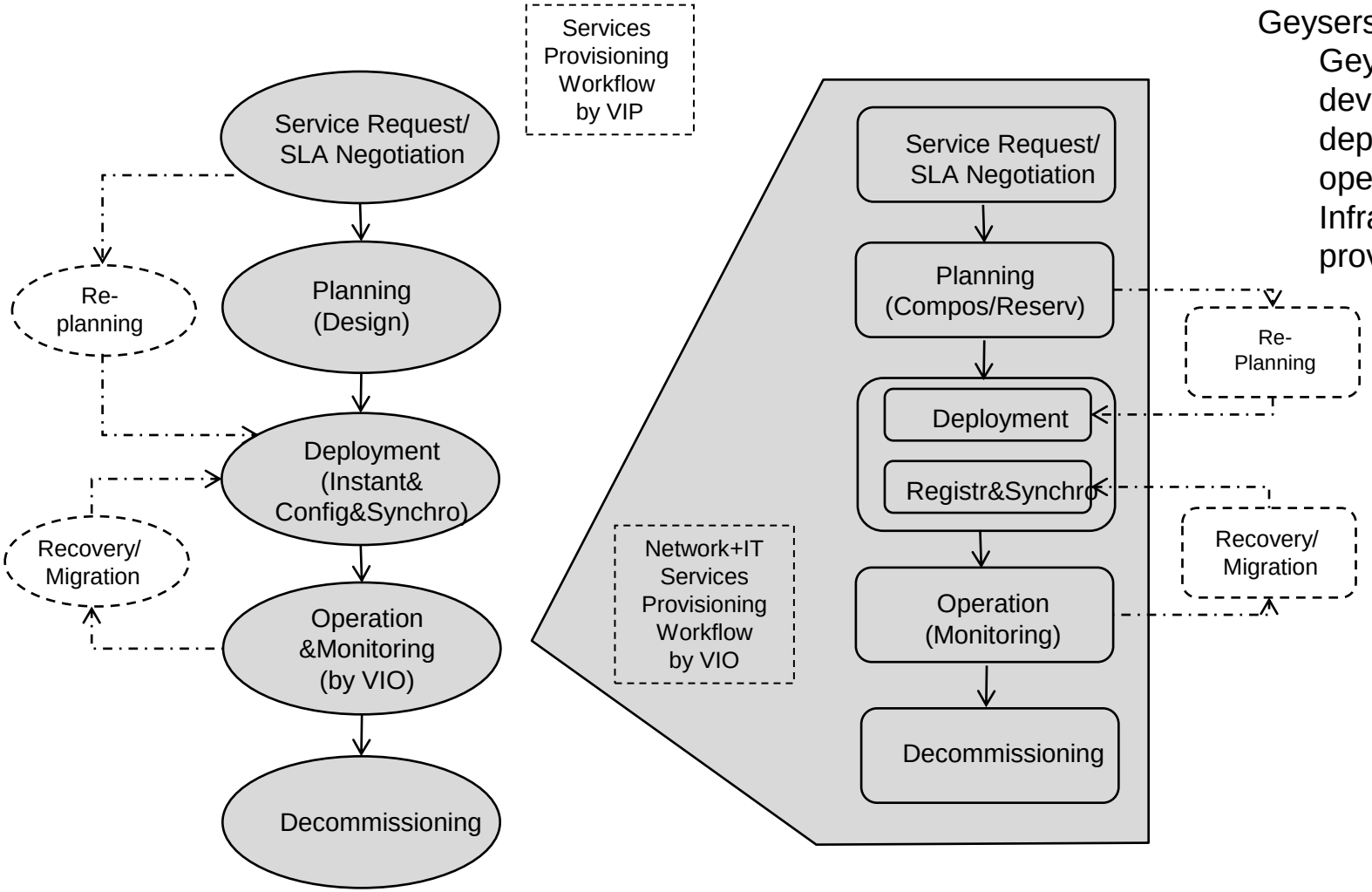
DEPLOYMENT stage

10 - Service Lifecycle Metadata Repository
11 - Service Lifecycle Metadata Coordinator
17 - Service Deployment Management

OPERATION stage

5 - Service Provisioning Management
6 - Service Quality/Problem Management
7 - Service Usage Monitor
12 - Service State Monitor
13 - Service Resource Fulfillment
14 - Service Resource Monitor
15 - Resource Usage Monitor

GEYSSERS Service Delivery Workflow



Geysers SDF supports both Geysers infrastructure development and deployments and its operation for on-demand Infrastructure services provisioning by VIO

SDF main stages and phases

Main stages/phases

- Service Request (including SLA negotiation)
- Planning (including Composition, Reservation and Design)
- Deployment (including Reqistration/Synchronisation)
- Operation (including Monitoring)
- Decommissioning

Additional stages

- Re-Composition should address incremental infrastructure changes
- Recovery/Migration can use SL-MD to initiate resources re-synchronisation but may require re-composition

The whole workflow should be supported by the Service Lifecycle Metadata Service (SL MD)

SDF use for defining Security Services Lifecycle Management Model

Security 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.

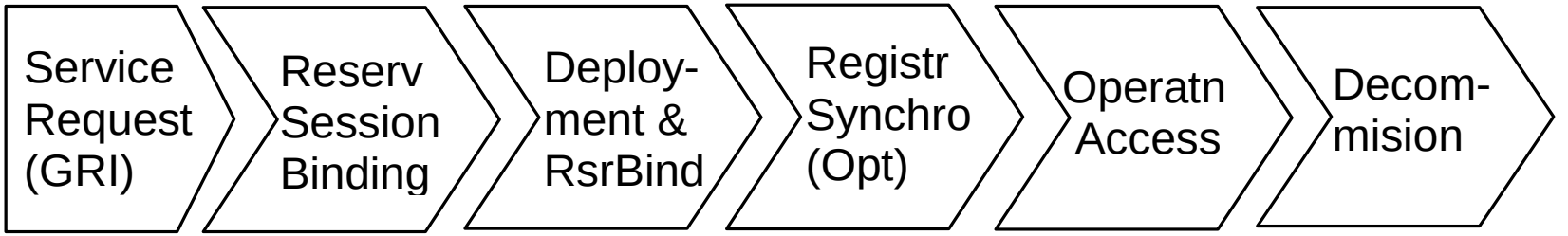
Reservation session binding that provides support for complex reservation process including required access control and policy enforcement.

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 GRI as a common provisioning session ID.

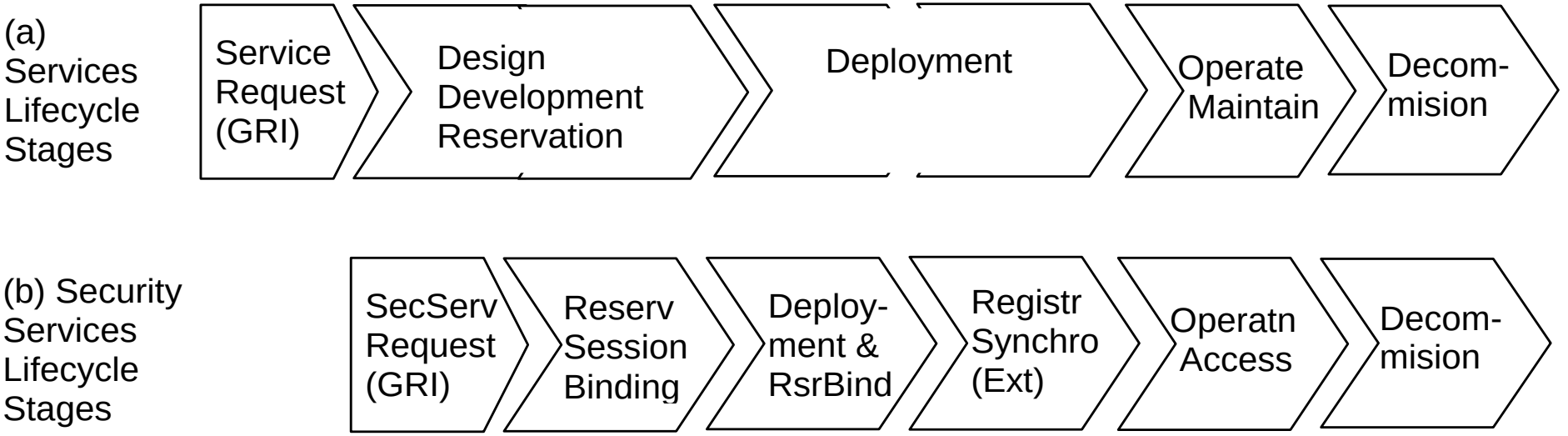
Registration&Synchronisation stage (optional) specifically targets possible scenarios with the provisioned services migration or failover/interruption. In a simple case, the Registration stage binds the local resource or hosting platform run-time process ID to the GRI as a provisioning session ID.

Operation stage - 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.



Relation between SSLM and general SLM



- Service Request stage may include SLA negotiation
  - Security service instantiation may use SLA security context

Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Design/Reservation Development	Deployment	Operation	Decomissioning
Process/ Activity	SLA Nego tiation	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**

SSLM – Existing developments

- GAAA Toolkit Library with tickets/tokens handling functionality for security session context management
- GAAA-NRP (GAAA profile for Network Resource Provisioning)
- On-going work in GEYSERS project to develop Security Architecture for On-Demand Infrastructure Services provisioning
- Possible Contribution to planned ISOD RG
  - Visit ISOD BOF today 15:00-18:30 (no security discussions planned but …)
  - http://www.gridforum.org/gf/event_schedule/index.php?id=2099

Additional Information

- TMF SDF Lifecycle Management model

Discussion

- CSA is proposed as a possible deliverable for ISOD RG
- Who is interested to contribute?
- Any interested people to review and verify against other usecases?