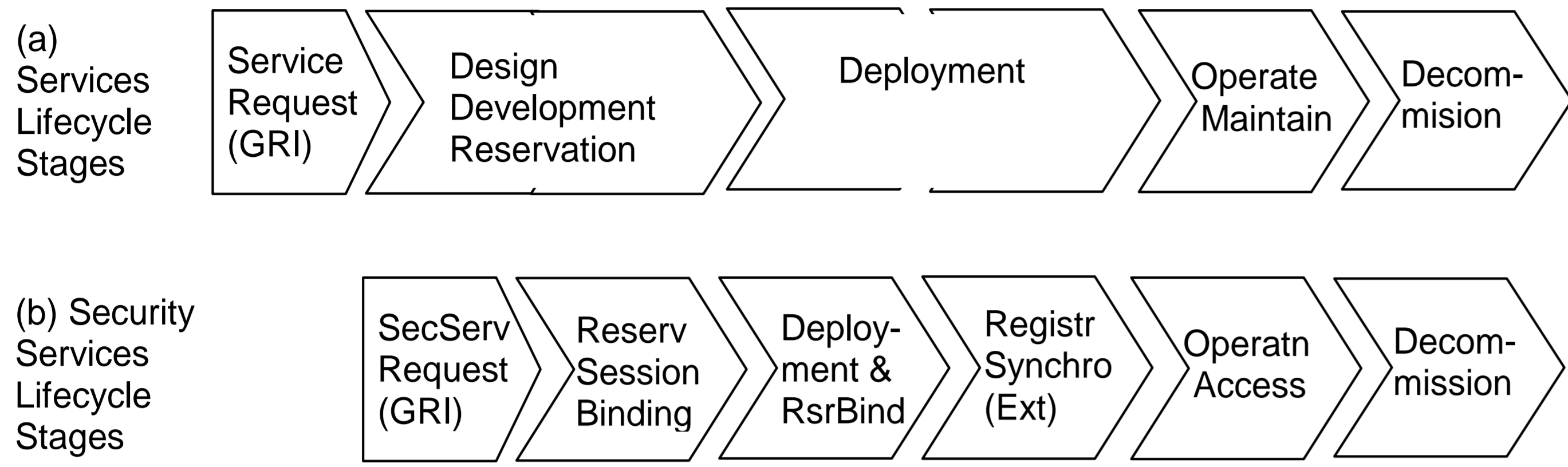


Security Services Lifecycle Management in Dynamically Provisioned Composable Services

Yuri Demchenko, Cees de Laat (University of Amsterdam), Diego R. Lopez (RedIRIS), Joan A. Garcia Espin (I2CAT)

Security Services Lifecycle 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.

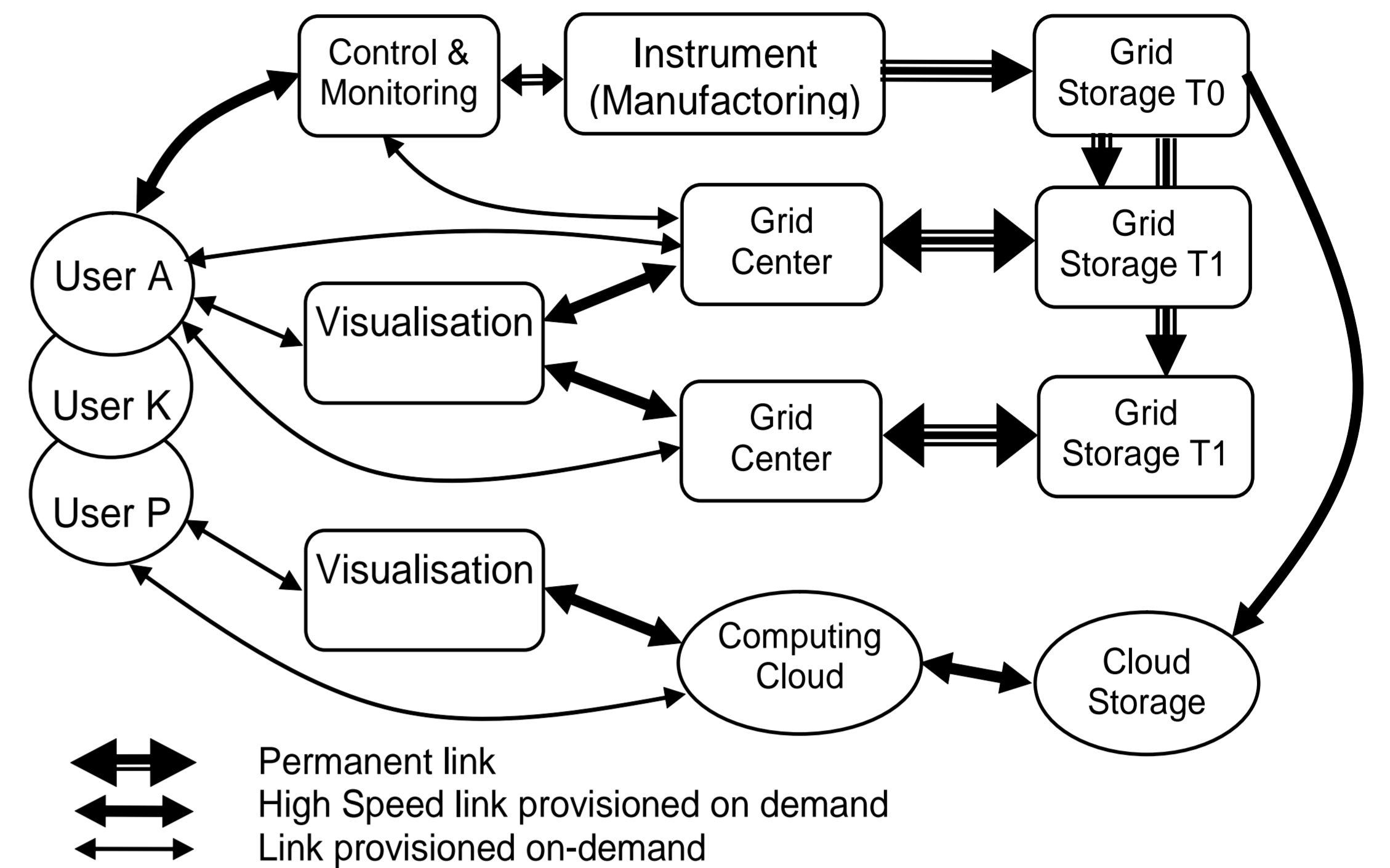
Deployment stage begins after all component resources have been reserved and includes distribution of the security context and binding the reserved resources or services to GRI as a common provisioning session ID.

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.

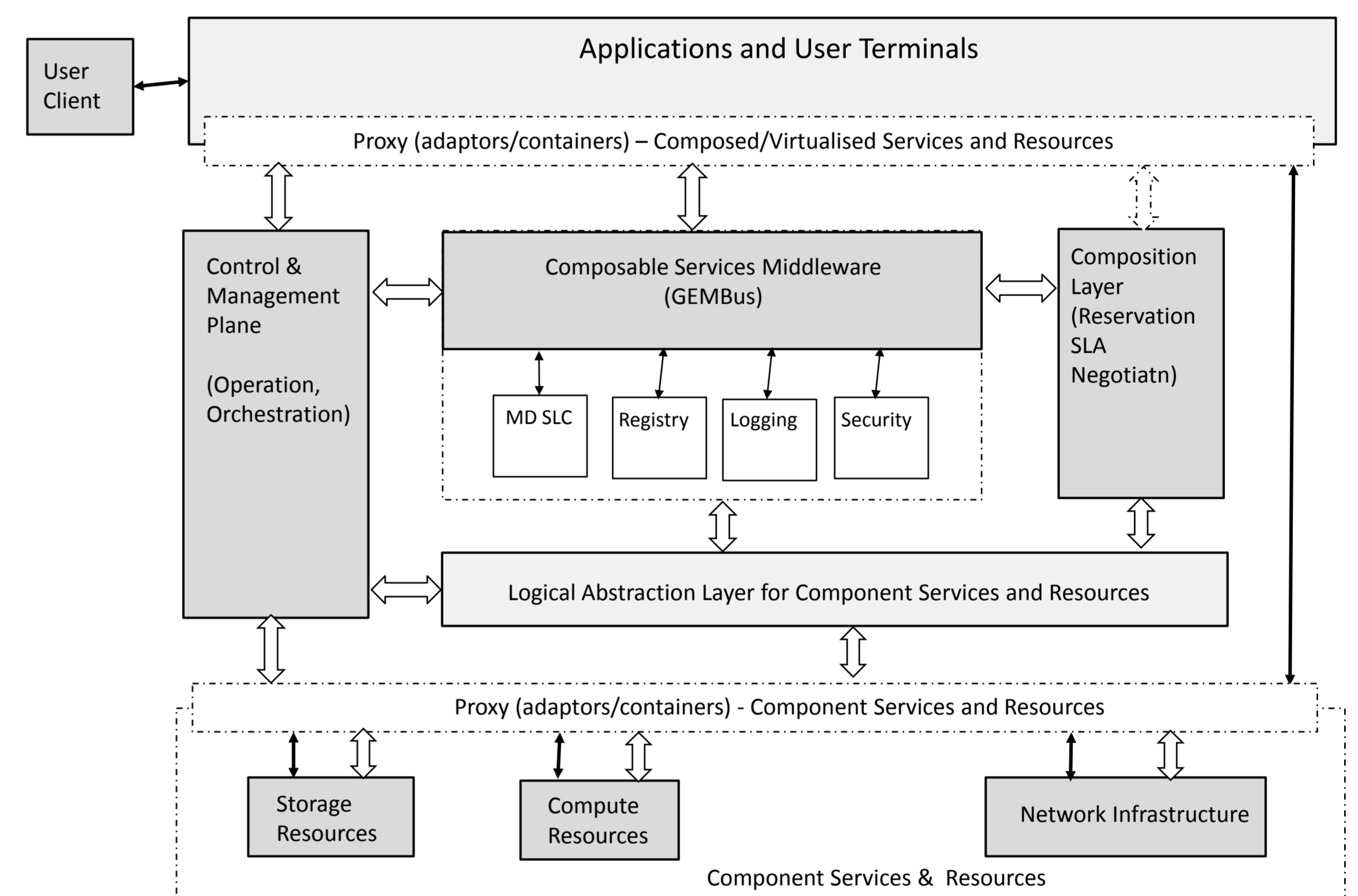
Decommissioning stage ensures that all sessions are terminated, data are cleaned up and session security context is recycled.

Use case: Provisioning Multi-domain Collaborative Environment On-Demand



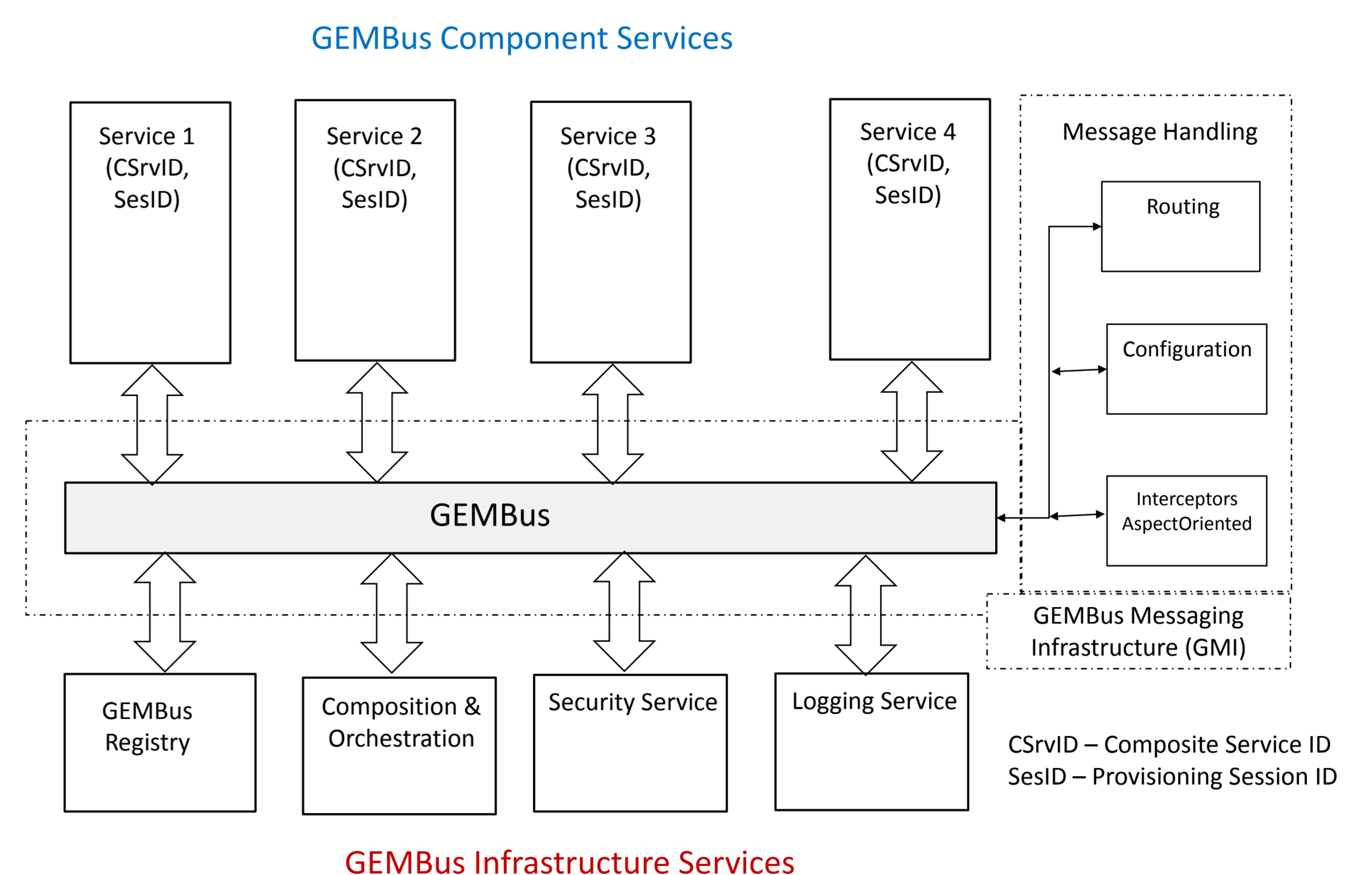
Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure.

Composable Services Architecture (CSA)



CSA Incorporates the major principles of the Service Oriented Architecture (SOA) and supports SLM/SSLM services lifecycle management models. Logical Abstraction layer provides a basis for uniform component services presentation allowing federated cross-domain composite services operation.

GEMBus Infrastructure for Composable Services



GEMBus provides common dynamically configurable messaging infrastructure for Composable services communication. GEMBus is an ongoing development in the GN3 JRA3 Task 3 Composable Services activity.

Contributing Project

GEANT3 JRA3 Task 3 – Composable services (GEMBus) - <http://www.geant.net/>
GEYSERS – Generalised Architecture for Infrastructure services - <http://www.geysers.eu/>

SLM stages	Request	Design/Reservation Development	Deployment	Operation	Decommissioning
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 Association		(V)	V	V	
AuthZ Session Context		V	(V)	V	
Logging		(V)	(V)	V	V

General and security mechanisms in SLM/SSLM

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.

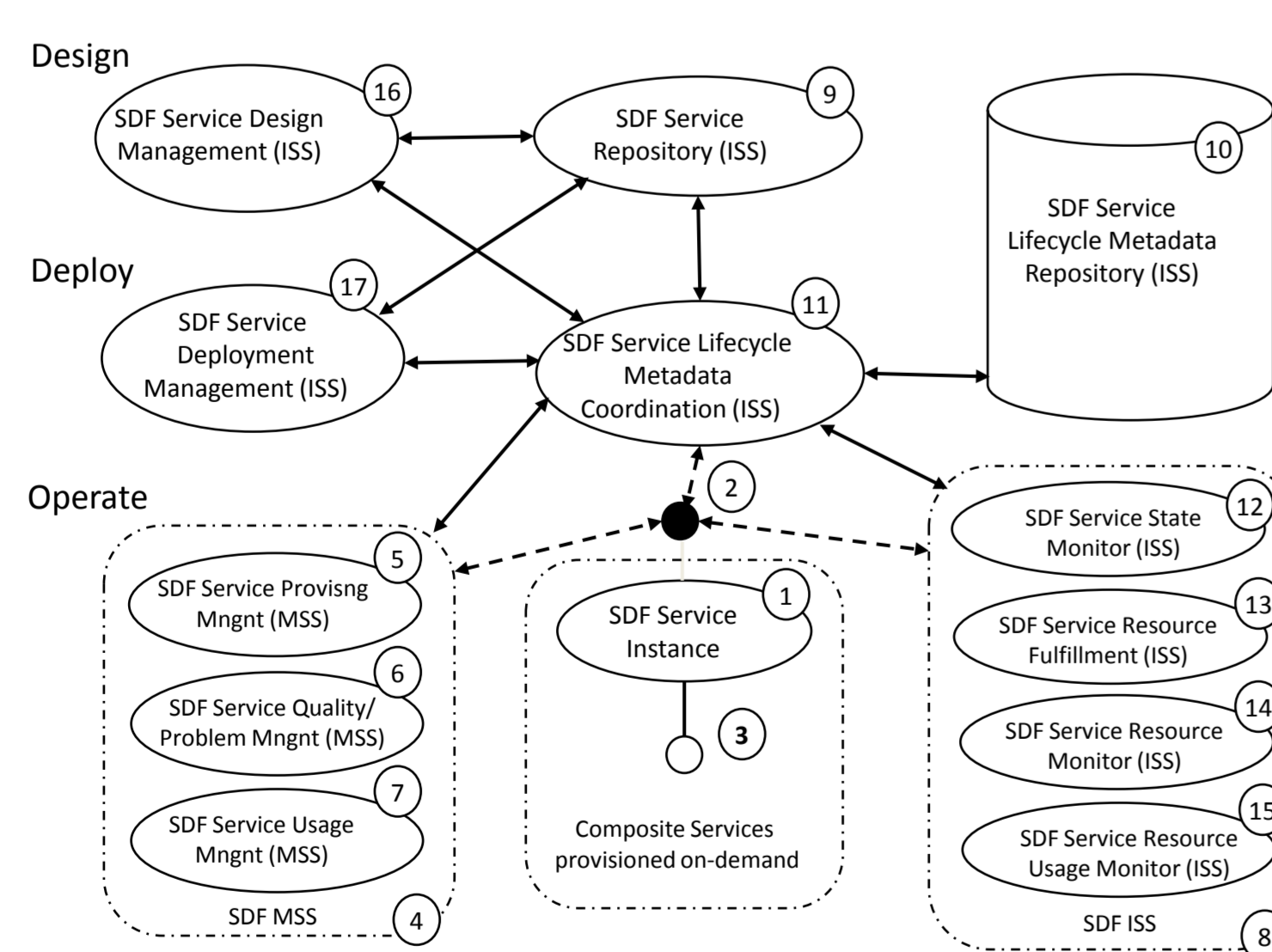
Authorisation Session Context supports integrity of the authorisation sessions during Reservation, Deployment and Operation stages.

Logging can be actually used at each stage and essentially important during the last 2 stages – Operation and Decommissioning.

Existing Frameworks in Services Virtualisation and On-Demand Provisioning

- ITU-T standards seria Y: Global information infrastructure, Internet protocol aspects and Next-Generation Networks (NGN)**
- ITU-T REC Y.2232 (01/2008) NGN convergence service model and scenario using Web Services
 - ITU-T REC Y.2234 (09/2008) Open service environment capabilities for NGN
 - ITU-T REC Y.2701 (04/2007) Security requirements for NGN release 1
 - Security requirements to NGN and security services binding to basic NGN interfaces (e.g., UNI, NNI, ANI)
- TMF standardised frameworks, practices and procedures**
- NGOSS – New Generation Operations Systems and Software (including eTOM)
 - SDF - Service Delivery Framework
 - SLAM - Service Level Agreement (SLA) Management Framework
- Open Group Service Integration Maturity Model (OSIMM)**
- Provides framework for evaluation and development of the strategy for business model/processes migration to true SOA
 - Defines 7 maturity level and 7 dimensions to achieve "Dynamically reconfigured virtualised services"
 - To ensure consistency security issues addressed at multiple dimensions: Business, Methods/models, Services. (Information)
- Microsoft Security Development Lifecycle (SDL) Framework**
- Primarily focused on the product development process by engineers/programmers
- (Training) – Requirements – Design – Implementation – Verification – Release – (Response)**

Service Delivery Framework (SDF) by TeleManagement Forum (refactored from[1])



Targeted automation of the whole service delivery and operation process including:

- 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

- 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

[1] TeleManagement Forum Service Delivery Framework (SDF) - <http://www.tmfforum.org/ServiceDeliveryFramework/4664/home.html>

Credits: Yuri Demchenko, Cees de Laat, Diego R. Lopez, Joan A. Garcia Espin
Contact: Yuri Demchenko <y.demchenko@uva.nl>