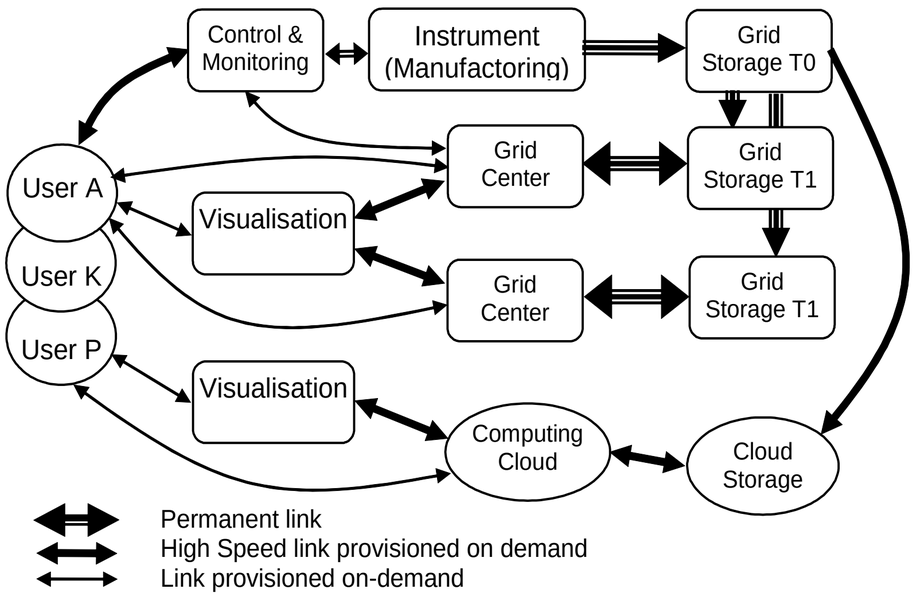
Composable Services Architecture (CSA) for Dynamically Configurable Virtualised Infrastructure Services Provisioning

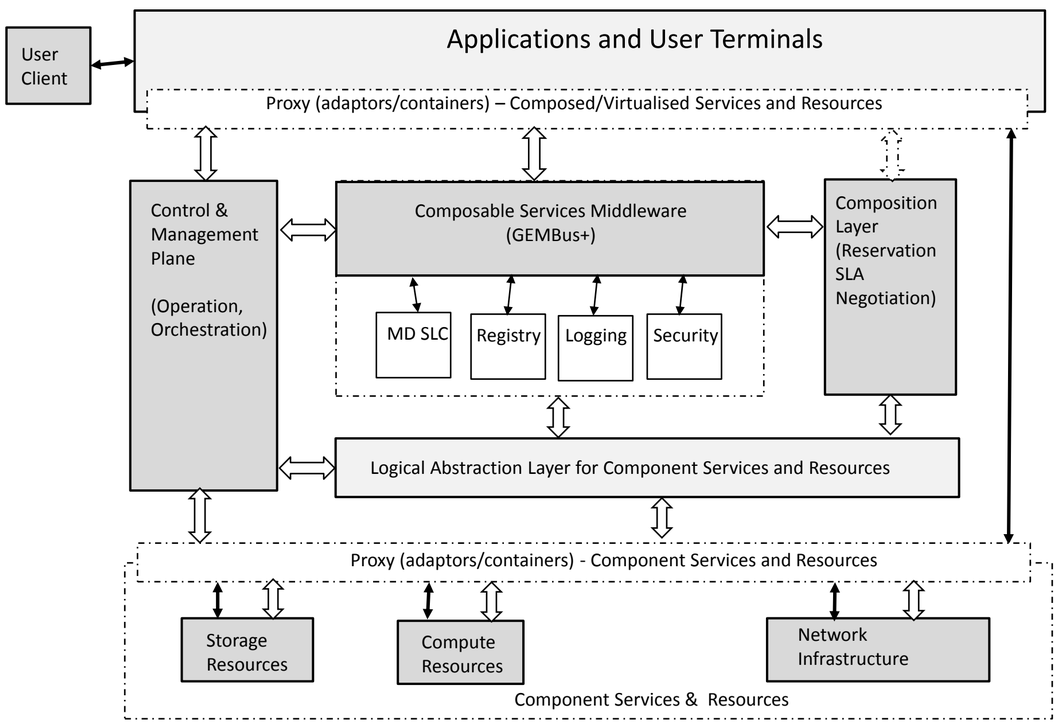
Yuri Demchenko, Cees de Laat (University of Amsterdam), Diego R. Lopez (RedIRIS), Joan A. Garcia Espin (I2CAT)

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



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

Composable Services Architecture (CSA)

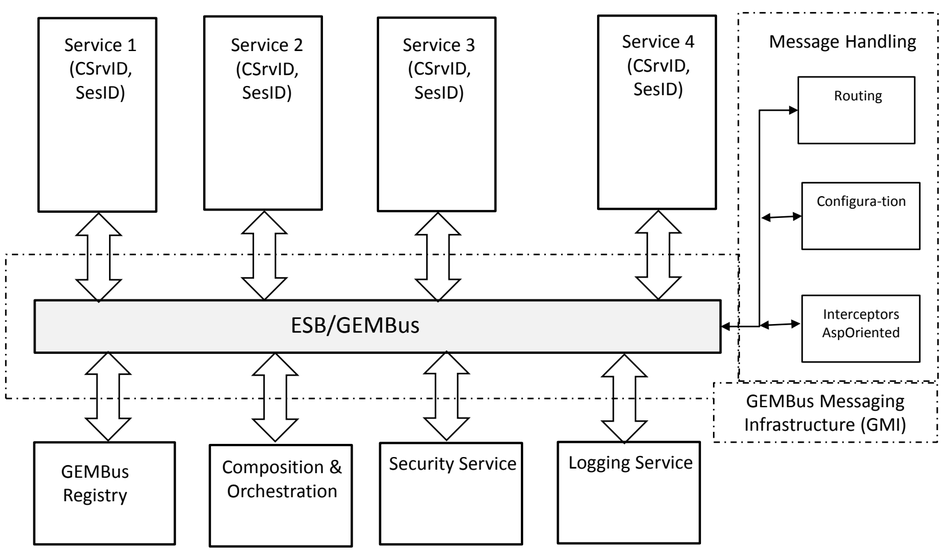


CSA Incorporates the major principles of the Service Oriented Architecture (SOA) and supports SLM/SSLM services lifecycle management models.

Logical Abstraction layer provides a basis for uniform component services presentation allowing federated cross-domain composite services operation.

GEMBus Infrastructure for Composable Services

GEMBus Component Services

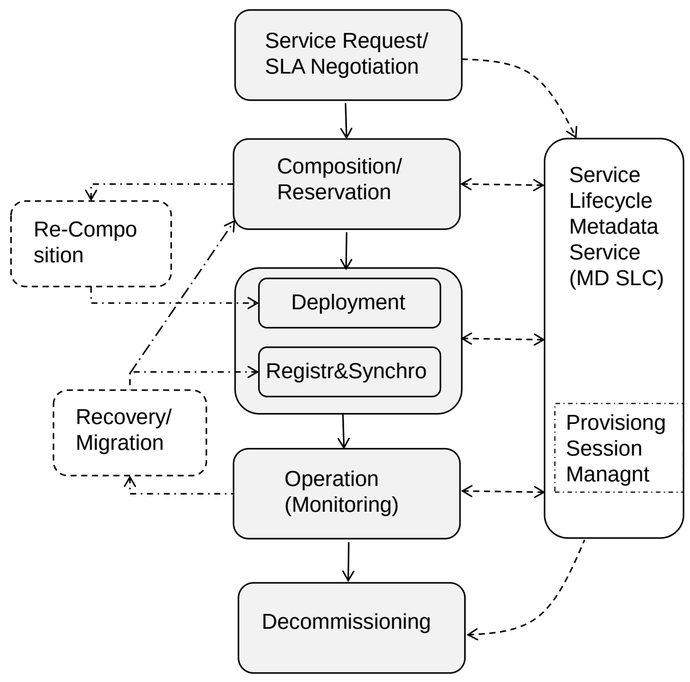


GEMBus Infrastructure Services

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.

Service Lifecycle Management (SLM) Model



Main stages

Service Request (including SLA negotiation). Global Reservation ID (GRI) is generated as a provisioning session identifier.

Planning (including **Composition** and **Reservation**) . May included SLA and access control policy enforcement.

Deployment. Component services configuration and initiation, including runtime binding to GRI.

Operation (including Monitoring) . Main operational stage of the provisioned services.

Decommissioning. All sessions are terminated, data are cleaned up and session security context is recycled.

Additional (sub-)stages

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

Recovery/Migration. Can use Service Lifecycle Metadata Service (MD-SLC) for services re-synchronisation or re-composition.

Security Services Lifecycle Management (SSLM) Model

SSLM includes additional stages to manage dynamic security associations and bind general provisioning session security context to virtualisation platform runtime environment:

- **Security Service Request** that initiates creation of the dynamic security association and may use SLA security context.
- **Reservation Session Binding** with GRI (as part of Planning stage) that provides support for complex reservation process including required access control and policy enforcement.
- **Registration&Synchronisation** stage (as part Deployment stage) specifically targets possible scenarios with the provisioned services migration and recovery.

Existing Frameworks for Services Virtualisation and On-Demand Provisioning

TMF standardised frameworks, practices and procedures
- NGOSS – New Generation Operations System and Software (including eTOM)
- SDF - Service Delivery Framework defining provisioned services lifecycle and corresponding infrastructure
- SLAM – SLA Management

ITU-T Next Generation Networks (NGN) Framework Y-seria standards
- 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

OSGi Service Framework that defines lower level component model for dynamically deployable managed Java based services that can be delivered and managed via network

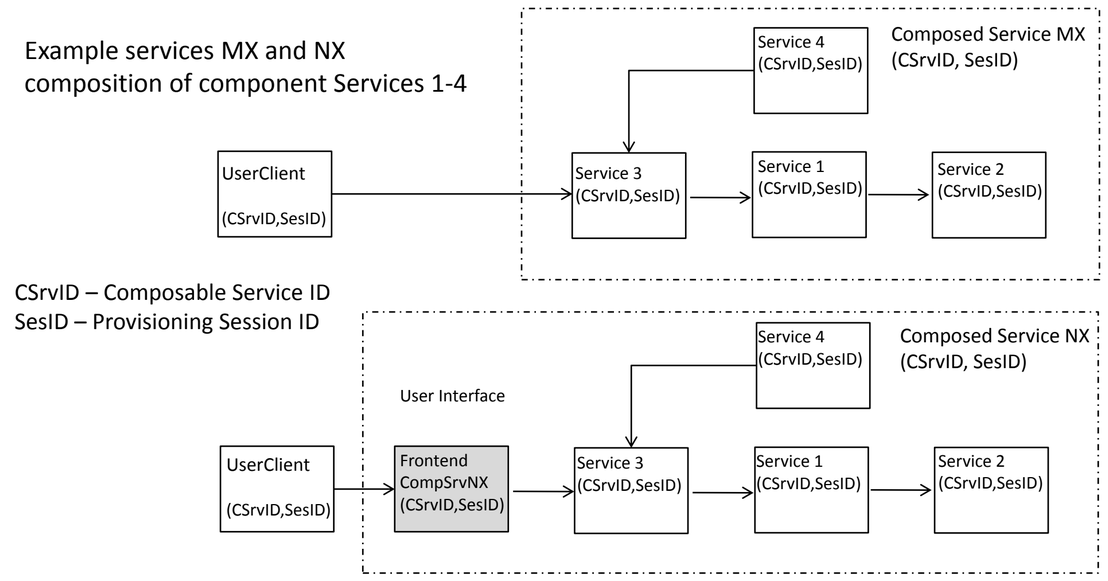
Open Systems Integration Maturity Model (OSIMM)
- Defines 7 maturity levels and 7 dimensions

Composable Services are defined in compliance with OSIMM as highest maturity level "Dynamically re-configured virtualised services", however requiring corresponding infrastructure.

Implementation Suggestions

GEMBus is being developed as CSA middleware and provides a platform for dynamic /on-demand services provisioning and management:
- Based on standard Enterprise Service Bus (ESB) implementations such as Fuse ESB (primary), SwordFish, Apache ServiceMix and corresponding service management components.
- Component services are created as OSGi services and deployed on the target GEMBus platform.
- SLM/SSLM implemented using OSGi lower level lifecycle management mechanisms and higher level BPEL environment that can be also implemented using other higher level workflow management frameworks.
- Security services are implemented using GEMBus Security Token Services (STS) and GAAA-Toolkit authorisation and security session management mechanisms that can be integrated with composable services using Spring Security framework both at bus level and at service level.

Example services MX and NX composition of component Services 1-4



Contributing Projects

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

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