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

(a) Services Lifecycle Stages

- Service Request (GR)
- Design Development Reservation
- Deployment
- Operate Maintain
- Decommission

(b) Security Services Lifecycle Stages

- SDF Service Request (GR)
- Reservation Binding
- Deploy & RedBind
-Registr (Syncroh) (Ext)
- Operate Access
- Decommission

Security Service request and generation of the GRI that will serve as a provisioning session identifier and will bind all other access 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 hosting platform run-time process ID to the GRI as a provisioning session ID.

Registration & Synchronization stage (optional) specifically targets possible scenarios with the provisioned services migration or failure/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 - service providers 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

GEMBus Infrastructure for Composable Service

GEMBus Component Services

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

Existing Frameworks in Services Virtualisation and On-Demand Provisioning

Existing Frameworks in Services Virtualisation and On-Demand Provisioning

- ITU-T standards series 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.2236 (09/2008) QoS provisioning and requirements for NGN
- ITU-T REC Y.2237 (03/2008) QoS provisioning and requirements for NGN
- ITU-T REC Y.2240 (06/2008) Security requirements for NGN
- ITU-T REC Y.2241 (09/2008) Security requirements to NGN and security services binding to basic NGN interfaces (e.g., UNI, NNI, ANI)
- NGOSS – New Generation (including eTOM)
- TMF standardised frameworks, practices and procedures
- GEMBus – New Generation (including SDX)
- Open Group Service Integration Maturity Model (OSIMM)
- NGSI2 – Next Generation Service Infrastructure
- SLM – Service Lifecycle Management
- SLA Management
- Open Group Service Integration Maturity Model (OSIMM)

GEMBus Infrastructure Services

GEMBus provides common dynamically configurable messaging infrastructure for Composable services communication

Contributing Project

GEEANT3 JRA3 Task 3 – Composable services (GEMBus) - http://www.geant.net/

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