# Security Infrastructure
for
# Cloud Infrastructure as a Service (IaaS) Provisioning Model

Yuri Demchenko

SNE Group, University of Amsterdam

Cloud Security Workshop

10-11 January 2011, Stavanger

# Outline

- System and Network Engineering group at University of Amsterdam
- Security Services Models Evolution
  - Evolution of the Generic AAA Authorisation Architecture
  - Security in Clouds – main issues
- Architectural Framework of the Cloud IaaS Provisioning Model
  - Composable Services Architecture (CSA)
  - Service Delivery Framework (SDF)
  - Infrastructure Services Modeling Framework (ISMF)
- Cloud Security and Dynamic Security Services Provisioning
- GEMBus as CSA middleware

- Additional information (GEYSERS AAI, GAAA-NRP, TMF SDF, ITU-T NGN)

# System and Network Engineering Group at University of Amsterdam

- SNE group is primarily a research group but also supports SNE master education
- Main research areas
  - High speed optical networks
    - Recent testbed achieved sub-40Gbps at Amsterdam-CERN link
  - Information modeling for network description
    - Extending to general IT resources
  - Security and generic AAA Authorisation framework (GAAA-AuthZ)
    - Evolving from client/security model to dynamically provisioned services
- Long term research cooperation with SURFnet and GigaPort programs in NL
- Re-building own testbed for optical network technologies and AAA/Security
- Recent and current projects participation – DatGrid, NextGrid, EGEE, Phosphorus, GEYSERS, GEANT3, NOVI
- Interest to Cloud technologies as an emerging common method to access complex infrastructure services – network and IT resources
  - Defining corresponding security models and infrastructure

# Security Services aspects/goals

- ✓ Access Control (including AuthN, AuthZ, Identity Management)
- ✓ Trust Management (including key management)
- ✓ Policy Based Management (PBM)
- ➢ Data protection (Confidentiality, Integrity, Access Control)
- – Communication Security
- – Privacy (complex of measures and policy based access control)

# Security Services Evolution

- Security services have dual task:
  - Protecting/ensuring normal/secure system operation
  - Protecting/providing secure access to system services and resources

- From the beginning of computer technologies the security services evolved from implicit/completely integrated with the program or computer to the composable components of the SOA based systems
  - Gradually revealing their duality

# Security Services Evolution – until late 1960s

Computer technology and Security services evolution

- Mechanical to Electronic calculators with simple input/output form
  - Simple calculation process control is programmed as a part of the program by using switches and stacks
  - Program execution is managed and controlled by user/programmer
    - No specific security services except physical security
  - Examples: Calculator, Turing Machine
- Mainframe computers with single task execution in time sharing mode
  - Simple Task monitor loads tasks/jobs in a scheduled sequence
  - Security services
    - Physical access control via terminals which can be also physically protected
    - Remote terminals may use hardware data/communication protection

# Security Services Evolution – until 1990s

- Multi-user and multi-task mainframe computers
  - Operating System performs programs, tasks and input/output functions/devices management
    - Multi-user and multi-task OS and Multi-user terminals
  - Security services are applied and managed by OS itself
    - Provide tasks (and user) isolation at the OS level
    - User access is controlled with the remote terminal protocols
    - First abstract security models: Reference Monitor, Bell-LaPadula, Biba, Clark-Wilson, Multi-Level Security (user clearance vs Data Sensitivity), RBAC
  - Overall security model is defined as the Trusted Computing Base (TCB)
- Distributed systems, Open Systems, Internet
  - Inter-computer communication, OSI, Internet, TCP/IP, Client/Server model
  - Two basic security models: TCB and OSI Security
    - Security services are decoupled from the main services and defined as such that can be called by other services to protect their normal operation
    - OSI Security Architecture proposed and standardised: ISO7498-2, ITU-T X.800 - defining multi-layer security services and mechanisms

# Security Services Evolution – late 1990s – late 2009

- Web based services, Web Services, Service Oriented Architecture (SOA)
  - Growing amount of service, information accessed via Internet
  - SOA facilitate services decomposition and decoupling of security services
    - Client/server model is changed to Requestor/Provider
    - SOA defines message based protocols (on the top of TCP/IP stack) – SOAP or REST/HTTP based
  - Computer security is provided by OS and network security is provided by user/terminal clients or services
    - SOA/WS security model is conformant to OSI/Internet security model by adding WS related upper message layer security
    - Security services are applied and managed separately by Security Management System
    - Definition of the Trusted Computing Platform Architecture (TCPA)
- Grid Computing
  - Cooperative resources sharing for Collaborative groups called Virtual Organisations (VO)
    - Open Grid Services Architecture (OGSA) is Web Services based with defined Job management/execution framework
  - OGSA Security architecture is VO and Web Services based
    - Security architecture attempts to bridge two basic security models: OSI/Internet user access and job submission security and TCB based job execution security
    - Security sessions context management becomes explicit task and require special mechanisms (protocols and credentials/assertions or security tokens)

# Security Services Evolution – since approx 2008

- Next Generation Network (NGN) and SOA based Enterprise Computing models
  - Network and IT services convergence based on SOA and Web Services
  - Addresses service virtualisation and on-demand provisioning
    - Enterprise Service Bus (ESB) as environment for dynamically re-configured virtualised composable services
    - Definition of the Service Delivery Framework (SDF) defining both the on-demand provisioned services lifecycle and service delivery and operation supporting infrastructure and business model
  - Federated access control to distributed multidomain services and resources
    - Security services are becoming dynamically composable services however (manually) pre-configured
    - Dynamic security association and security context management in multidomain environment
    - Security services lifecycle management as composable services
- Emerging Cloud Computing
  - Emerging as a common access method to complex infrastructure services/resources provisioned on-demand
    - (Infrastructure, Platform, Software) as a Service provisioning models
    - Services and resources are based on virtualisation
    - Services are provisioned on demand and typically require/follow standard Service Delivery workflow
    - There is no well-defined  architecture frameworks yet
  - **There is  no well defined security model or security architecture**
    - Security paradigm change due to the fact that user data are processed  in uncontrolled  for user environment
    - Current security model is based on SLA contracted between user and provider  and enforced by provider
    - Require solutions/mechanisms to enable trusted remote platform for users
    - Security context and lifecycle management
    - Prospective security architecture should support  both dynamic provisioning environment and dynamic security services provisioning
    - Potentially interest will return to using Trusted Computing Platform Architecture
    - Promising/emerging research on homomorphic/elastic encryption (recently proposed by Stanford Univ.)

# GAAA-AuthZ Development Stages (1)

- Defined in RFC2904 - RFC2906
  - Redefines OSI X.812 Authorisation Framework for Internet protocols
  - Addresses multi-domain issues and session management
- Authorisation for web based services and Web Services
  - Authorisation session context management with AuthZ tickets
  - User-centric security model for multi-domain multilayer collaborative environment
  - Implementation in Collaboratory.nl
- Authorisation for Grid/OGSA and Web Services
  - Security context and Authorisation session management in multi-tier environment combining Internet user access and TCB/UNIX based job execution environment
  - VO based security federations and attributes management in multi-domain collaborative environment
  - Common XACML/SAML attributes profile for authorisation in Grid
  - Implementation in EGEE and gLite Authorisation Framework

# GAAA-AuthZ Development Stages (2)

- Generic AAA Authorisation framework for multidomain Network Resource Provisioning - GAAA-NRP profile
  - Authorisation session and security context management in multidomain environment during the whole provisioning process
    - Access and pilot tokens for access control and signaling
  - Dynamic trust association creation and management
  - Common XACML/SAML attributes profile for NRP
  - Implementation in Phosphorus
- Security infrastructure for on-demand infrastructure services provisioning
  - Extended security context management and GAAAPI interfaces
    - Dynamic policy generation and federated attributes management
    - Dynamic trust associations and security property information modeling
  - Security Services Lifecycle Management (SSLM) model and supporting mechanisms
  - Projects - GEYSERS and GN3-JRA3 Composable Services
- On-demand provisioned virtualised security services and infrastructure
  - Security infrastructure for Cloud IaaS provisioning infrastructure
  - Dynamic security services provisioning and security infrastructure virtualisation

# SNE @ UvA take on Cloud technology

- Defining architectural framework for Cloud Infrastructure as a Service (IaaS) provisioning model
  - Consistent security architecture can only be built if the main system/services/infrastructure are well defined
- Dynamically configured security services/infrastructure
- OGF On-Demand Infrastructure Service (ISOD) provisioning BoF/RG
  - Including definition of IaaS and required security models

# Cloud Security – Issues and problem environment

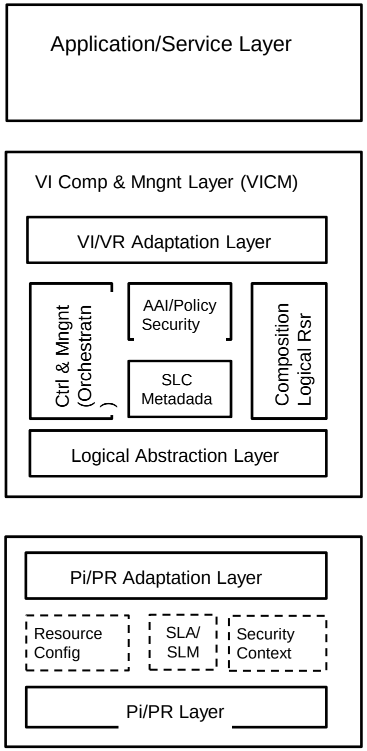
- Virtualised services
- On-demand/dynamic provisioning
- Multi-tenant/multi-user
- Multi-domain
- Uncontrolled execution environment
  - Data protection
    - Trusted Computing Platform Architecture (TCPA)
    - Promising homomorphic/elastic encryption
- Integration with legacy security services/infrastructure of the providers
- Integration with the providers business workflow

# Proposed Architectural Framework for Cloud IaaS

The proposed framework should support on-demand infrastructure services provisioning and operation

- **Composable Services Architecture (CSA)** that intends to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services
- **Service Delivery Framework (SDF)** that provides a basis for defining the whole composable services life cycle management and supporting infrastructure services
- **Infrastructure Services Modeling Framework (ISMF)** that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring
- (Optionally) ***Service Control and Management Plane/Framework*** may be defined as combination of management functionality in all 3 components
- ***Security services/infrastructure*** have a dual role:
  - Virtual Security Infrastructure - provisioned as a part of virtualised infrastructure
  - Support normal/secure operation of the whole provisioning framework

# IaaS General Model



Application/Service Layer

VI Comp & Mngnt Layer (VICM)

VI/VR Adaptation Layer

Ctrl & Mngnt (Orchestratn)

AAI/Policy Security

SLC Metadada

Composition Logical Rsr

Logical Abstraction Layer

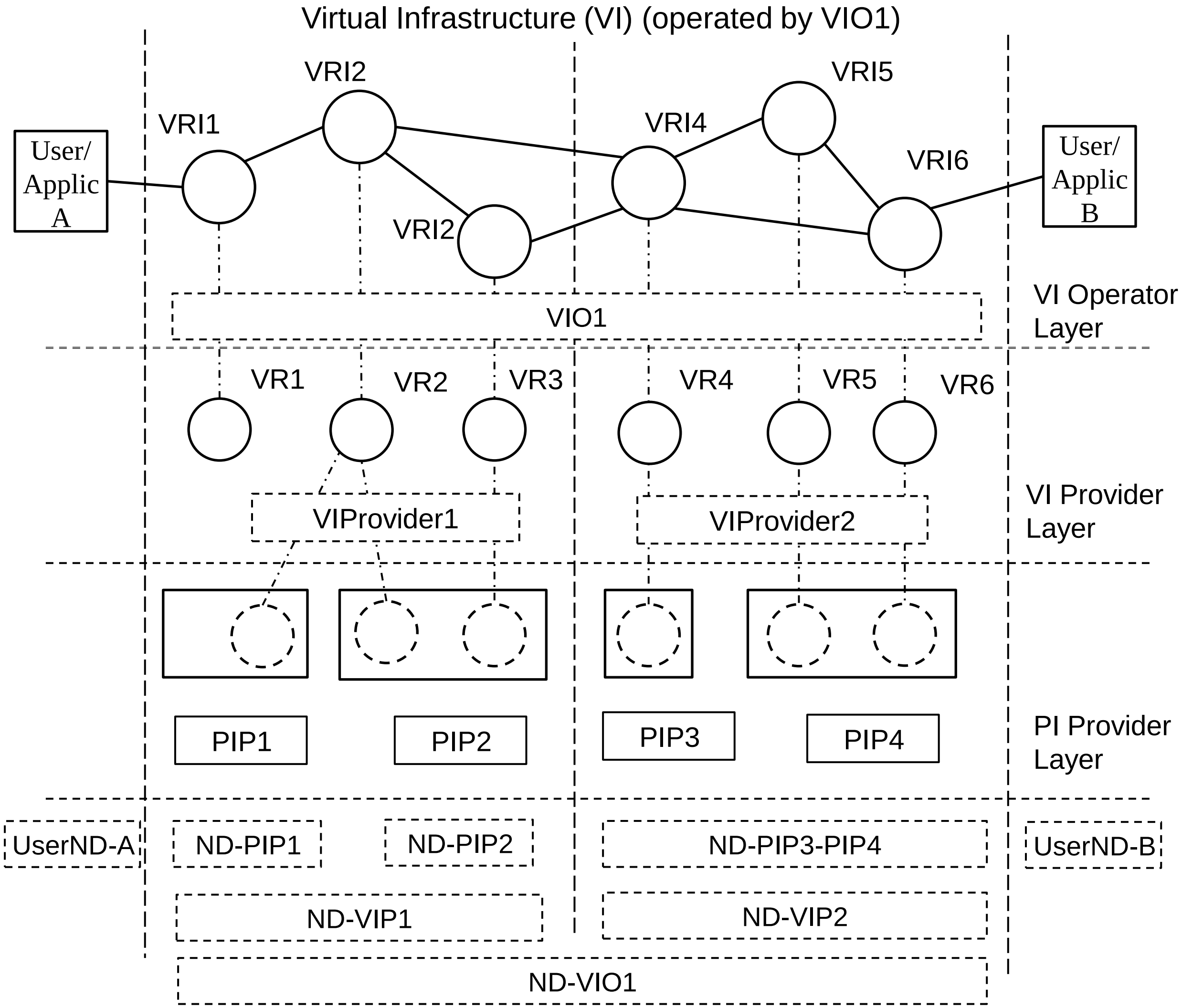
Pi/PR Adaptation Layer

Resource Config

SLA/ SLM

Security Context

Pi/PR Layer



Virtual Infrastructure (VI) (operated by VIO1)

User/ Applic A

VRI1

VRI2

VRI2

VRI4

VRI5

VRI6

User/ Applic B

VIO1

VI Operator Layer

VR1

VR2

VR3

VR4

VR5

VR6

VIProvider1

VIProvider2

VI Provider Layer

PIP1

PIP2

PIP3

PIP4

PI Provider Layer

UserND-A

ND-PIP1

ND-PIP2

ND-PIP3-PIP4

UserND-B

ND-VIP1

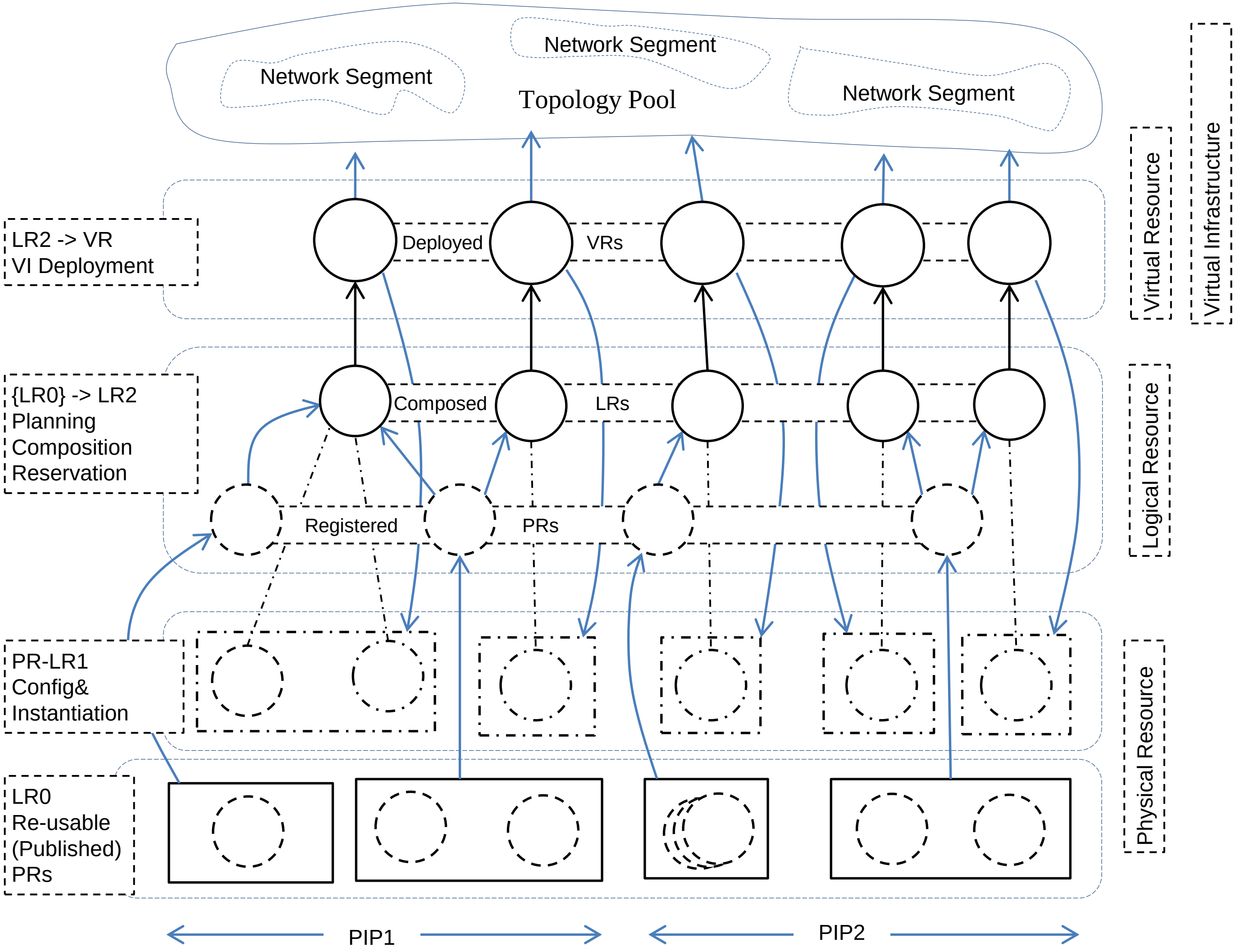
ND-VIP2

ND-VIO1

# Virtual Infrastructure Composition and Management (VICM) Layer Operation

- Main actors involved into provisioning process
  - Physical Infrastructure Provider (PIP)
  - Virtual Infrastructure Provider (VIP)
  - Virtual Infrastructure Operator (VIO)
- Virtual Infrastructure Composition and Management (VICM) layer includes
  - VICM middleware - defined as CSA
  - Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper Application layer.
- The infrastructure provisioning process includes the following main stages
  - (1) virtual infrastructure creation request
  - (2) infrastructure planning and advance reservation;
  - (3) infrastructure deployment including services synchronization and initiation;
  - (4) operation stage
  - (5) infrastructure decommissioning
- VICM redefines Logical Infrastructure Composition Layer (LICL) proposed by GEYSERS project
  - Basic functionality is implemented as GEMBus/CSA

# ISMF – Virtual Resource Lifecycle



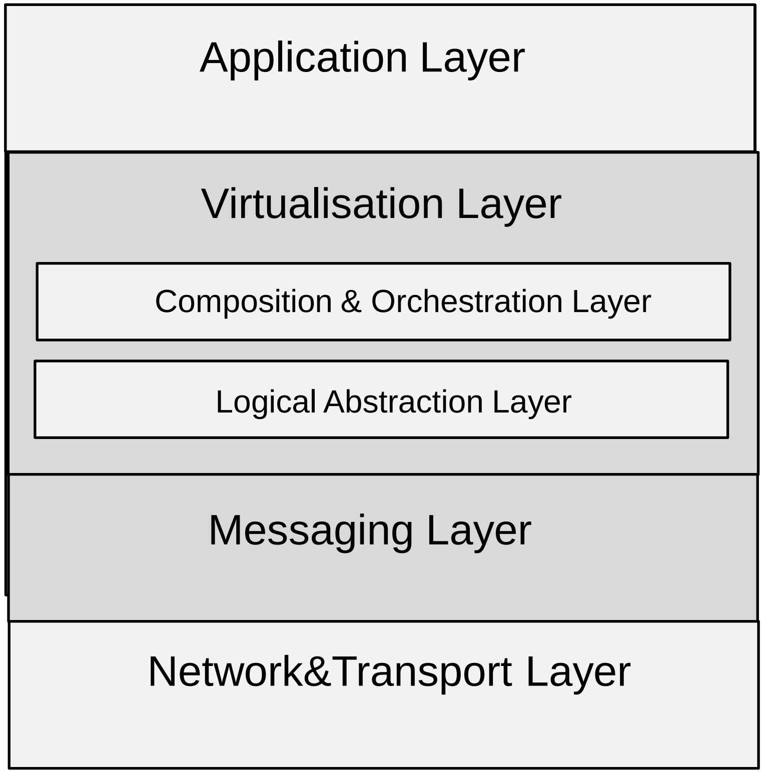
# ISMF - Relation between PR-LR-VR-VI

- Virtual Resource lifecycle – defines relations between different resource presentations along the provisioning process
- Physical Resource information is published by PIP to the Registry service serving VICM and VIP
  - Logical Resource representing PR includes also properties that define possible (topological) operations on the PR, such as e.g. partitioning or aggregation.
- Published LR information presented in the commonly adopted form (using common data or semantic model) is then used by VICM/VIP composition service to create requested infrastructure as combination of (instantiated) Virtual Resources and interconnecting them with the available network infrastructure
- Network infrastructure can be composed of a few network segments (from the network topology pool) run by different network providers.
- Composed LRs are deployed as VRI/VI to VIP/VIO and as virtualised/instantiated PR-LR to PIP
- Resource/service description format considered
  - NDL/NML (Network Description Language / Network Markup Language at OGF)
  - USDL (Unified Services Description Language) at W3C
  - VXDL infrastructure service request format by INRIA

# Composable Services Architecture (CSA)

- Defined as middleware for on-demand provisioned Composable Services
- Proposed in the GEANT3 JRA3 Composable Services project
- Implemented as GEMBus (GEANT Multidomain Bus)

# Composable Services Layered Model



Application Layer

Virtualisation Layer

Composition & Orchestration Layer

Logical Abstraction Layer

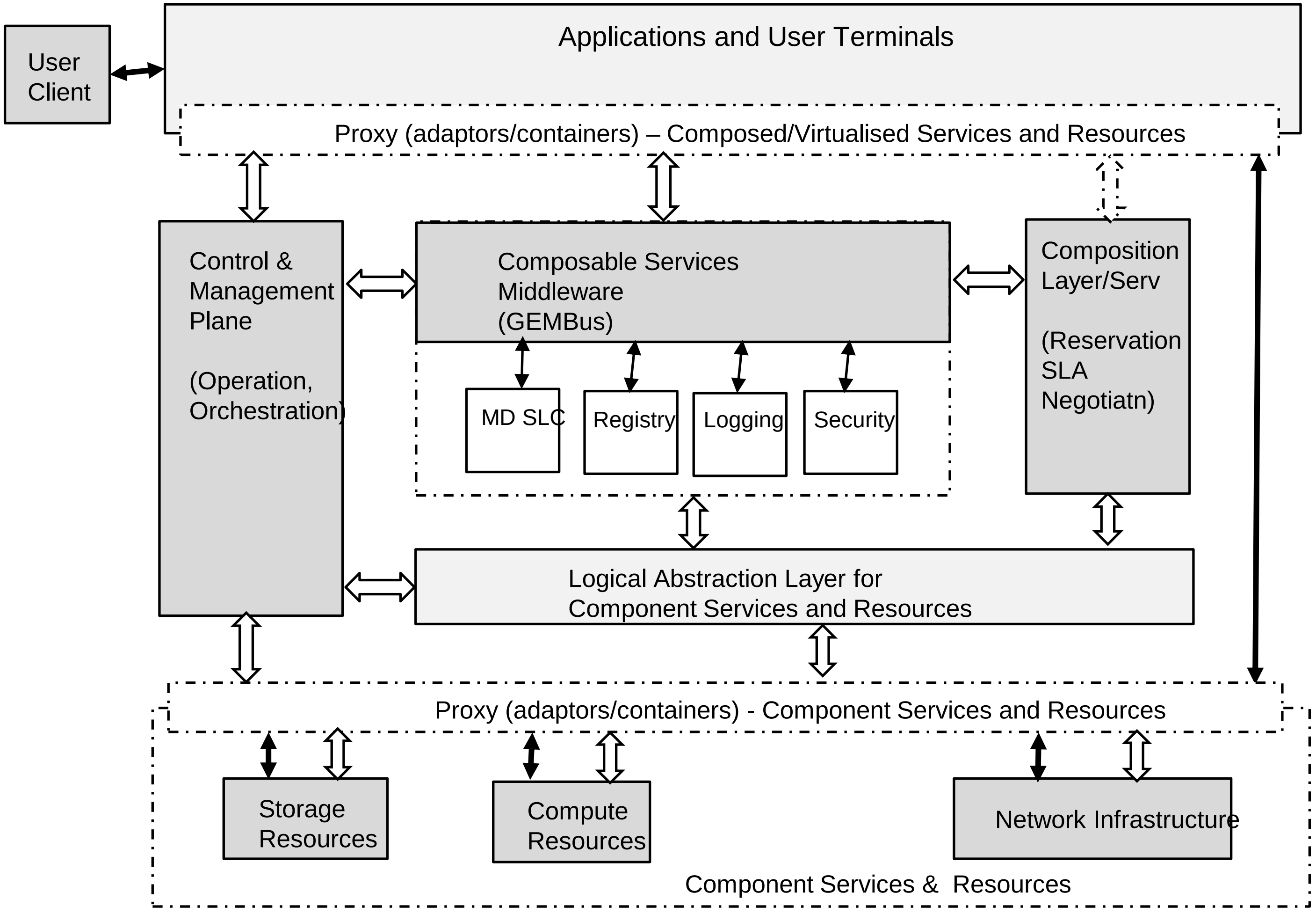
Messaging Layer

Network&Transport Layer

- Application Layer hosts application related protocols
- GEMBus Messaging Infrastructure (GMI) includes
  - Messaging Layer
  - Virtualisation (Composition&Orchestration) Layer
- Network&Transport Layer should allow using/binding to standards communication and security protocol

- Composable services are defined as ***“dynamically re-configured virtualised services”*** according to OSIMM model

# Composable Services Architecture – Version 0.13


User Client
Applications and User Terminals
Proxy (adaptors/containers) – Composed/Virtualised Services and Resources
Control & Management Plane
(Operation, Orchestration)
Composable Services Middleware (GEMBus)
MD SLC
Registry
Logging
Security
Composition Layer/Serv
(Reservation SLA Negotiatn)
Logical Abstraction Layer for Component Services and Resources
Proxy (adaptors/containers) - Component Services and Resources
Storage Resources
Compute Resources
Network Infrastructure
Component Services & Resources

Composable Services lifecycle/provisioning stages

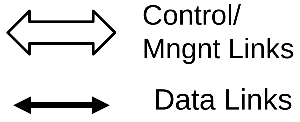
(1) Request

(2) Composition/ Reservation

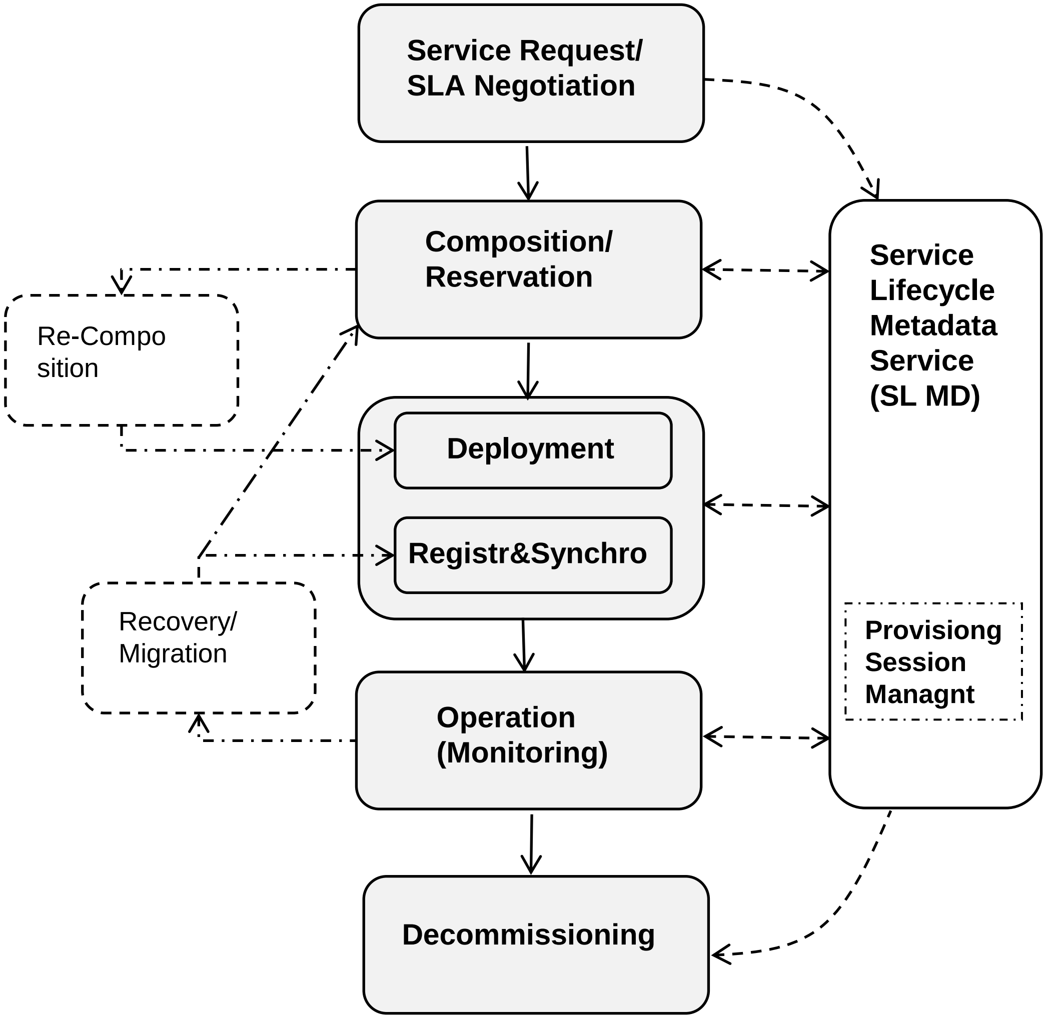
(3) Deployment

(4) Operation

(5) Decommissioning

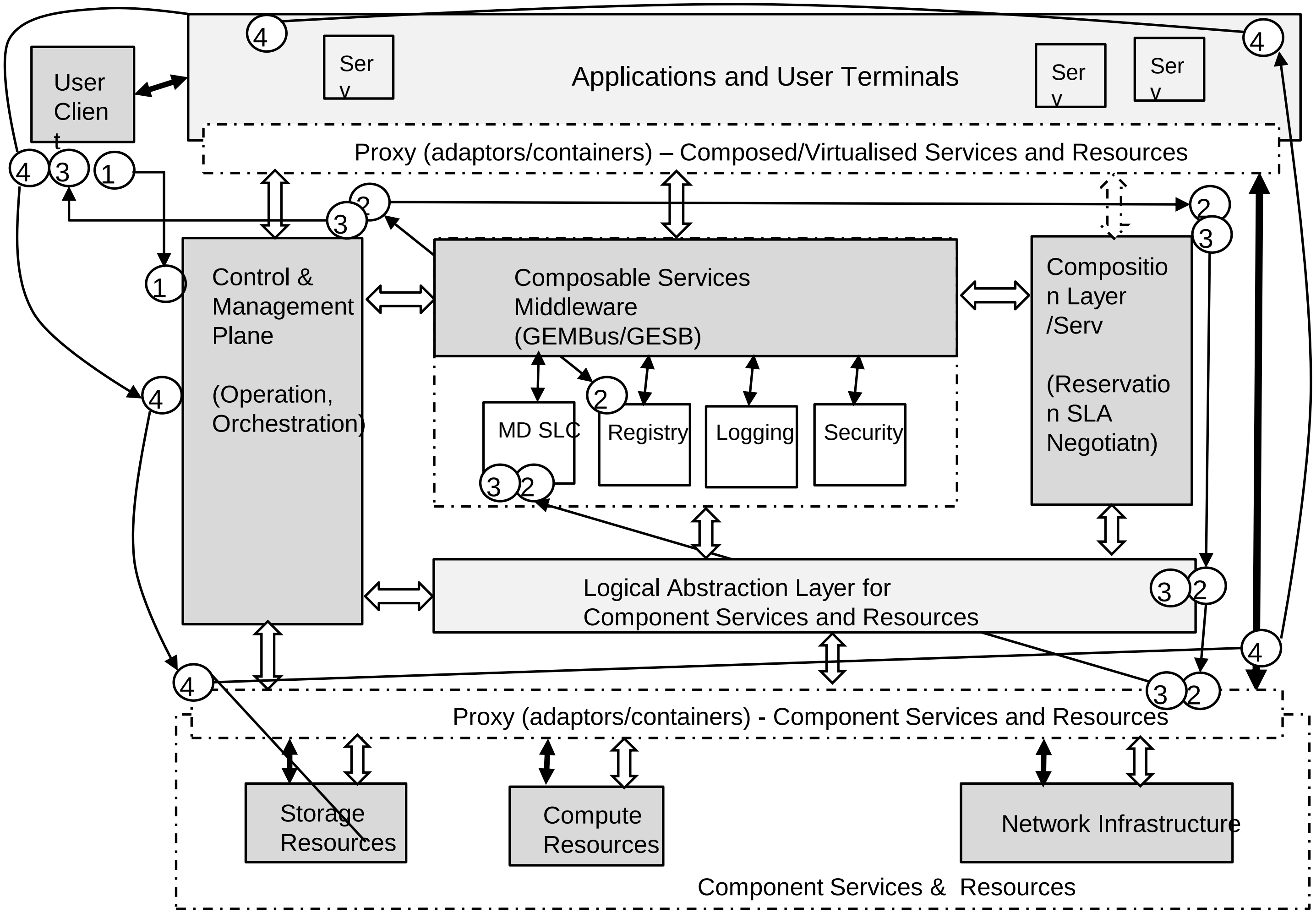


# Composable Services Lifecycle/Provisioning Workflow



- Main stages/phases
  - Service Request (including SLA negotiation)
  - Composition/Reservation (aka 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 is supported by the Service Lifecycle Metadata Service (SL MD)
-

# Composable Services Architecture – Version 0.13
# Lifecycle stages workflow


User Client
Applications and User Terminals
Serv
Serv
Serv
Proxy (adaptors/containers) – Composed/Virtualised Services and Resources
Control & Management Plane
(Operation, Orchestration)
Composable Services Middleware (GEMBus/GESB)
MD SLC
Registry
Logging
Security
Composition Layer /Serv
(Reservation SLA Negotiatn)
Logical Abstraction Layer for Component Services and Resources
Proxy (adaptors/containers) - Component Services and Resources
Storage Resources
Compute Resources
Network Infrastructure
Component Services & Resources
1
2
3
4

Composable Services lifecycle/provisioning stages
(1) Request
(2) Composition/ Reservation
(3) Deployment
(4) Operation
(5) Decommissioning

MD SLC – Service Lifecycle Metadata

GEMBus – GEANT Multidomain Bus

GESB – Geysers ESB

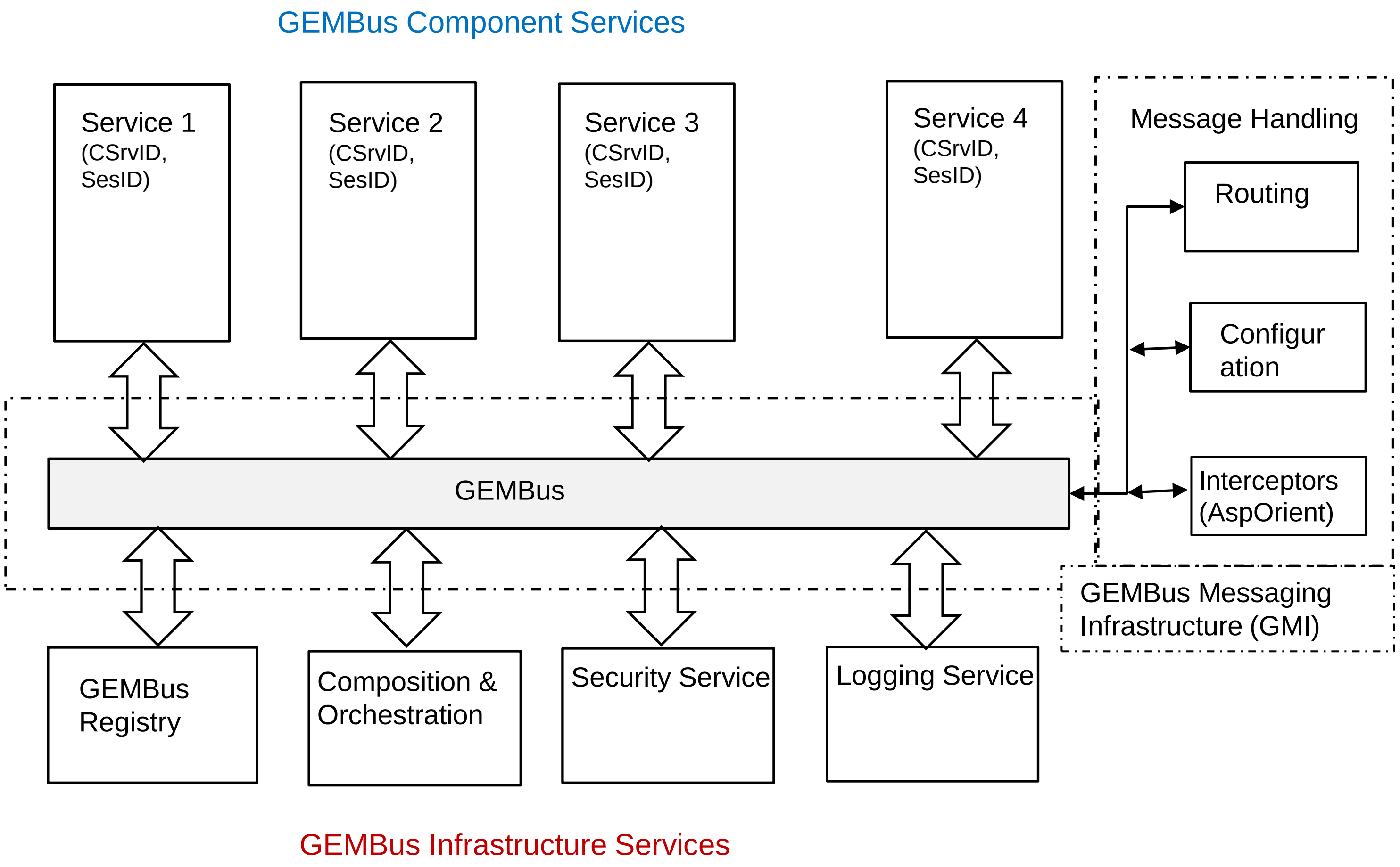
⇔ Control/ Mngnt Links

⟷ Data Links

# CSA functional elements interaction

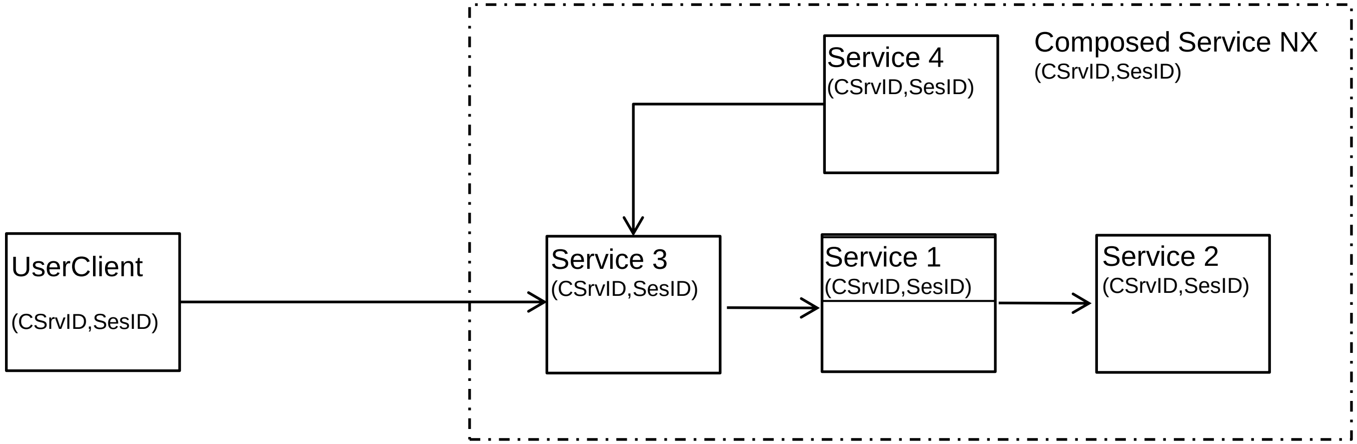
- **(1) Request**
  - User Client -> Control and Management
- **(2) Composition/ Reservation**
  - Control&Mngnt -> Registry -> Composition/Reservation Serv -> (Logical Abstract -> Resr Adapters) -> LC Metadata Serv
- **(3) Deployment**
  - Control&Mngnt -> Composition/Reservation Serv -> (Logical Abstract -> Resr Adapters) -> LC Metadata Serv -> User Client
- **(4) Operation**
  - User Client -> Control&Mngnt (Orchestration) -> Rsr Adapters -> Virtualised/Composed Applications
- **(5) Decommissioning**
  - Control&Mngnt -> LC Metadata Serv -> (Logical Abstract -> Resr Adapters)

# GEMBus Infrastructure for Composable Service


GEMBus Component Services
Service 1 (CSrvID, SesID)
Service 2 (CSrvID, SesID)
Service 3 (CSrvID, SesID)
Service 4 (CSrvID, SesID)
Message Handling
Routing
Configur ation
Interceptors (AspOrient)
GEMBus
GEMBus Messaging Infrastructure (GMI)
GEMBus Registry
Composition & Orchestration
Security Service
Logging Service
GEMBus Infrastructure Services

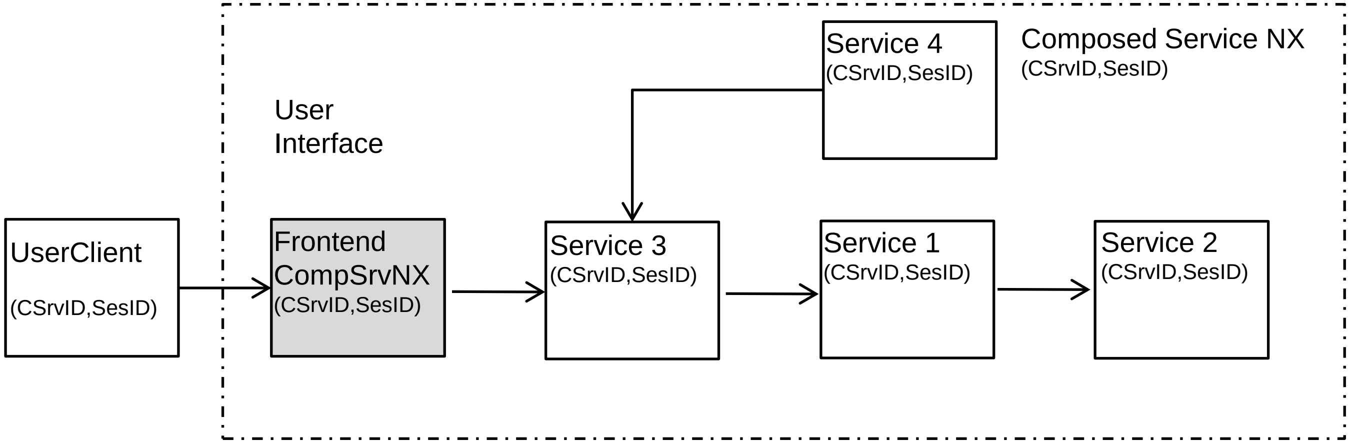
GEMBus provides common dynamically configurable messaging infrastructure for Composable services communication

# Example Service Composition – Service NX



Role and place for Composition and Orchestration

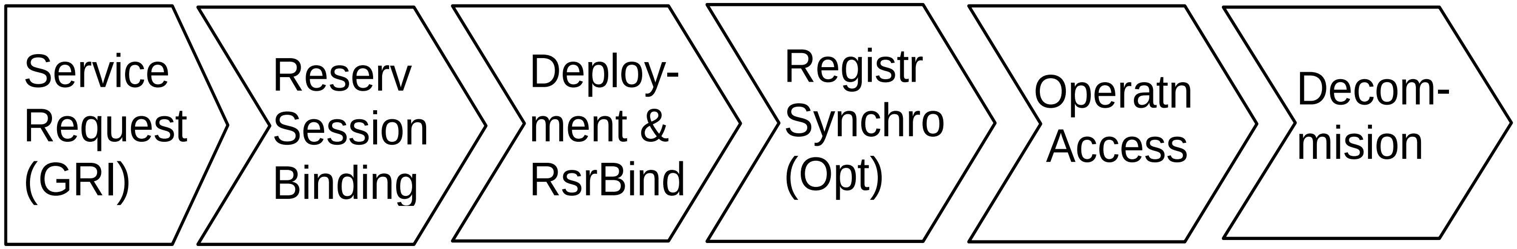
* Composable services or GEMBus infrastructure service



- CSrvID, SesID – bind component services into the on-demand provisioned Composed service NX

# Security Services Lifecycle Management (SSLM) Model

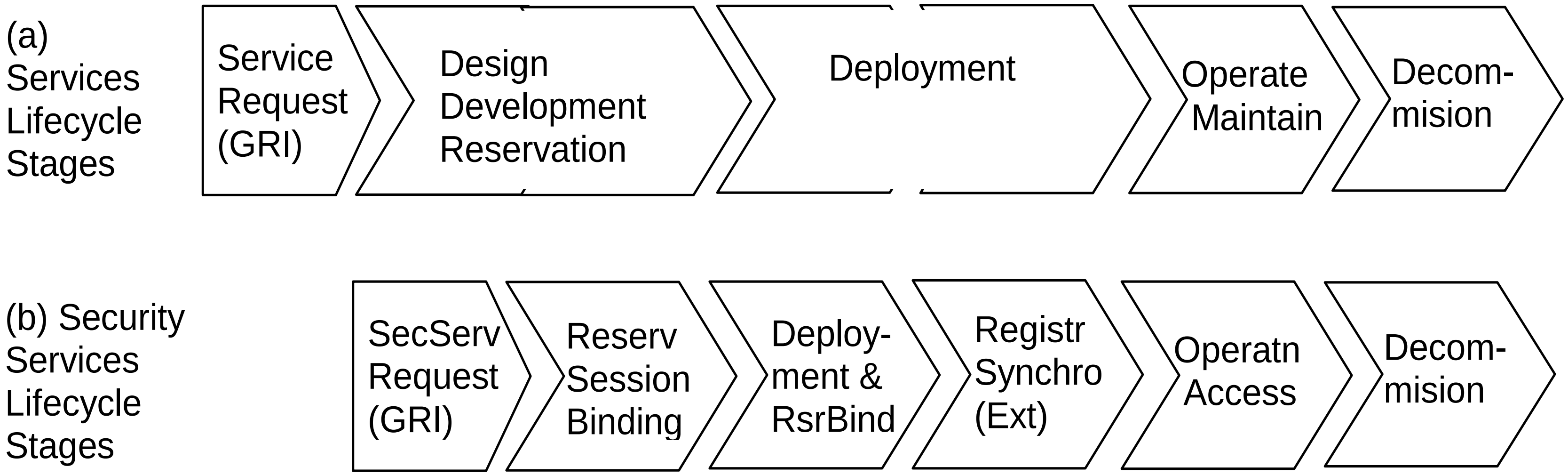
- **Security Service request and generation of the GRI** that will serve as a provisioning session identifier and will bind all other stages and related security context.
- **Reservation session binding** that provides support for complex reservation process including required access control and policy 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/SLM stages and supporting general and security mechanisms

| SLM stages | Request | Design/Reservation 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 | |
| Metadata | V | V | V | V | |
| Dynamic Security Associatn | | (V) | V | V | |
| AuthZ Session Context | | V | (V) | V | |
| Logging | | (V) | (V) | V | V |

# Relation between SSLM and general SLM



(a) Services Lifecycle Stages

Service Request (GRI) → Design Development Reservation → Deployment → Operate Maintain → Decom-mision

(b) Security Services Lifecycle Stages

SecServ Request (GRI) → Reserv Session Binding → Deploy-ment & RsrBind → Registr Synchro (Ext) → Operatn Access → Decom-mision

Specific SSLM stages and mechanisms to ensure consistency of the security context management

- **Security Service Request** that initiates creation of the dynamic security association and may use SLA security context.
- **Reservation Session Binding** with GRI (also a part of general SDF/SLM) that provides support for complex reservation process including required access control and policy enforcement.
- **Registration&Synchronisation** stage (as part Deployment stage) that allows binding the local resource or hosting platform run-time process ID to the GRI as a provisioning session ID. Specifically targets possible scenarios with the provisioned services migration or restoration.

# Possible next steps

- Possible EU project
  - Can be both general Cloud problems and Cloud Security
  - May combine both infrastructure services and security
- ISOD BoF/RG at OGF31 (22-25 March 2011, Taipei, Taiwan)
  - Cloud Security BoF at OGF31
  - Additionally, special session on Cloud related topic at OGF31
- Workshop on Cloud Security at CloudCom2011 in Athens
- SECOTS2011 Workshop at CTS2011 (22-26 May 2011, Philadelphia, USA)
- Possible other meeting events: CLOSER2011/NL, Cloud Workshop at INFOCOM2011/Changhai, CLOUD2011 in Washington

# Additional Information

- SDF Lifecycle Management model
- GAAA-NRP Operation and provisioning process
- Using AuthZ tickets and tokens for access control and signaling
- ITU-T NGN Open Service Environment

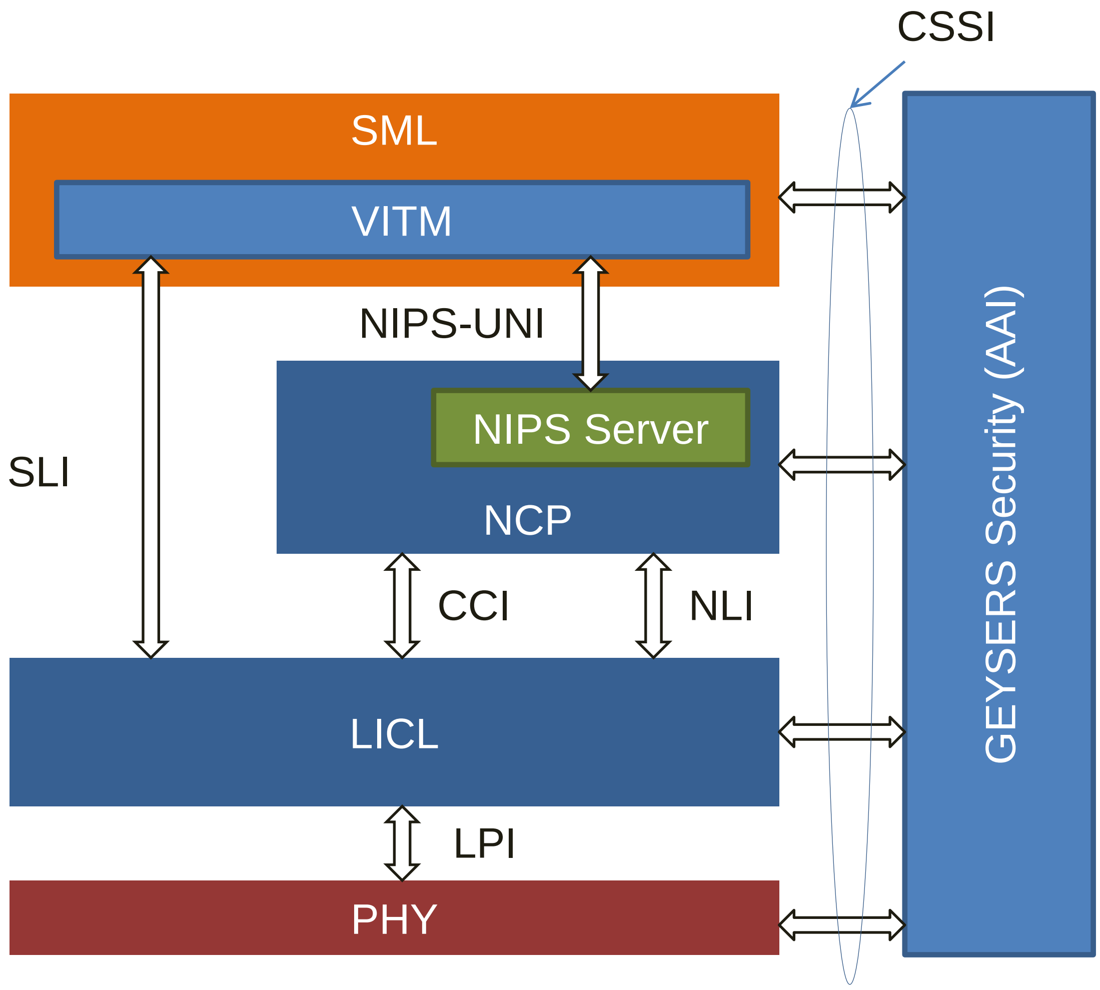
# AAI in GEYSERS (1)

Authentication and Authorization Infrastructure (AAI) functionalities

- Access control: interfaces, VI provisioning service
  - Authentication – standard implementation
  - Authorization – primary focus
  - Identity management – to support multi-domain attributes management
- Security context management for VI provisioning service
  - Cross-layer/multi-layer
  - Inter-domain/dynamic security associations
  - Lifecycle and provisioning session security context
- Dynamic access control services/infrastructure
  - Security Services Lifecycle Management (SSLM)
  - Dynamic security/trust associations management

.

# AAI in GEYSERS (2)

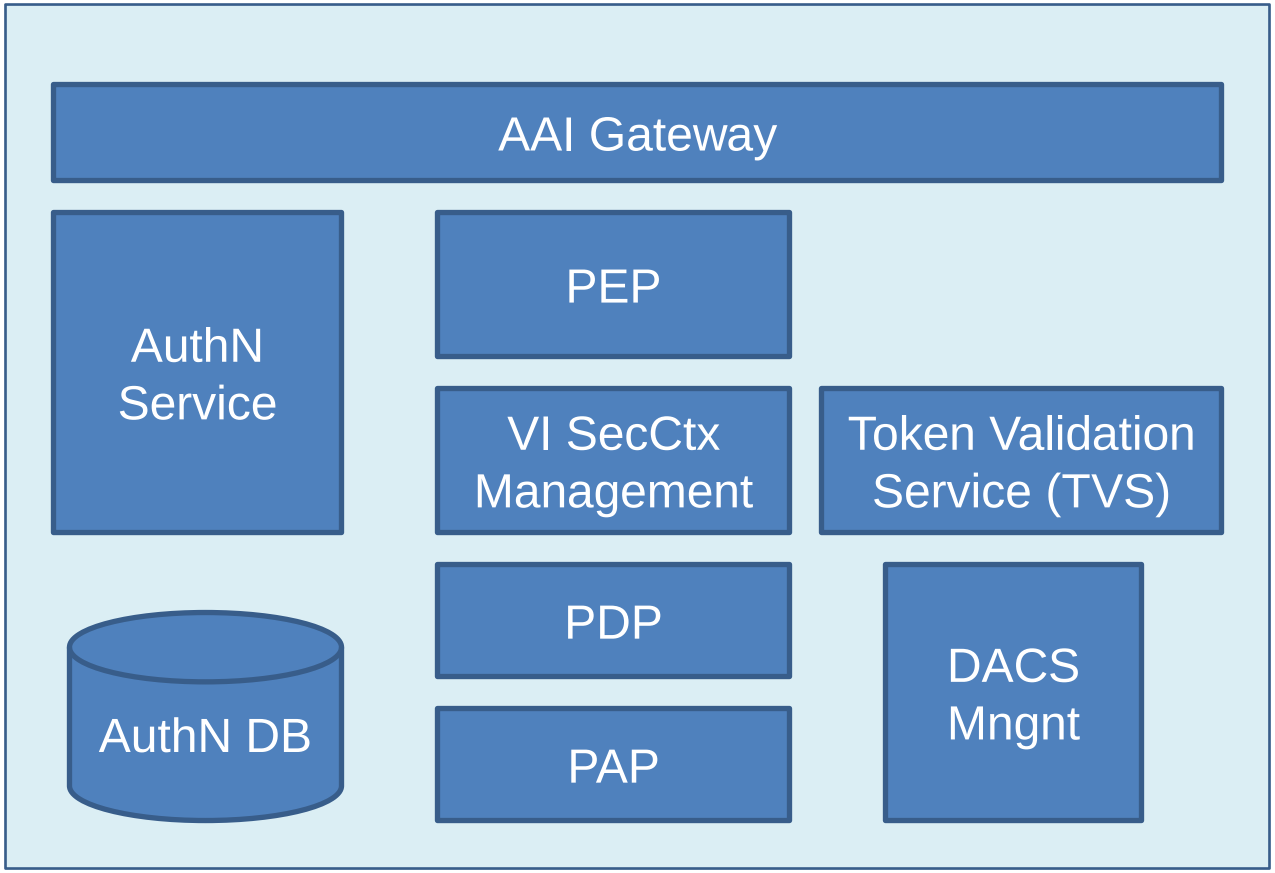


Basic CSSI services

- Data encryption
- Digital signature
- Authentication
- Authorization
- Policy management
- Security session and context management

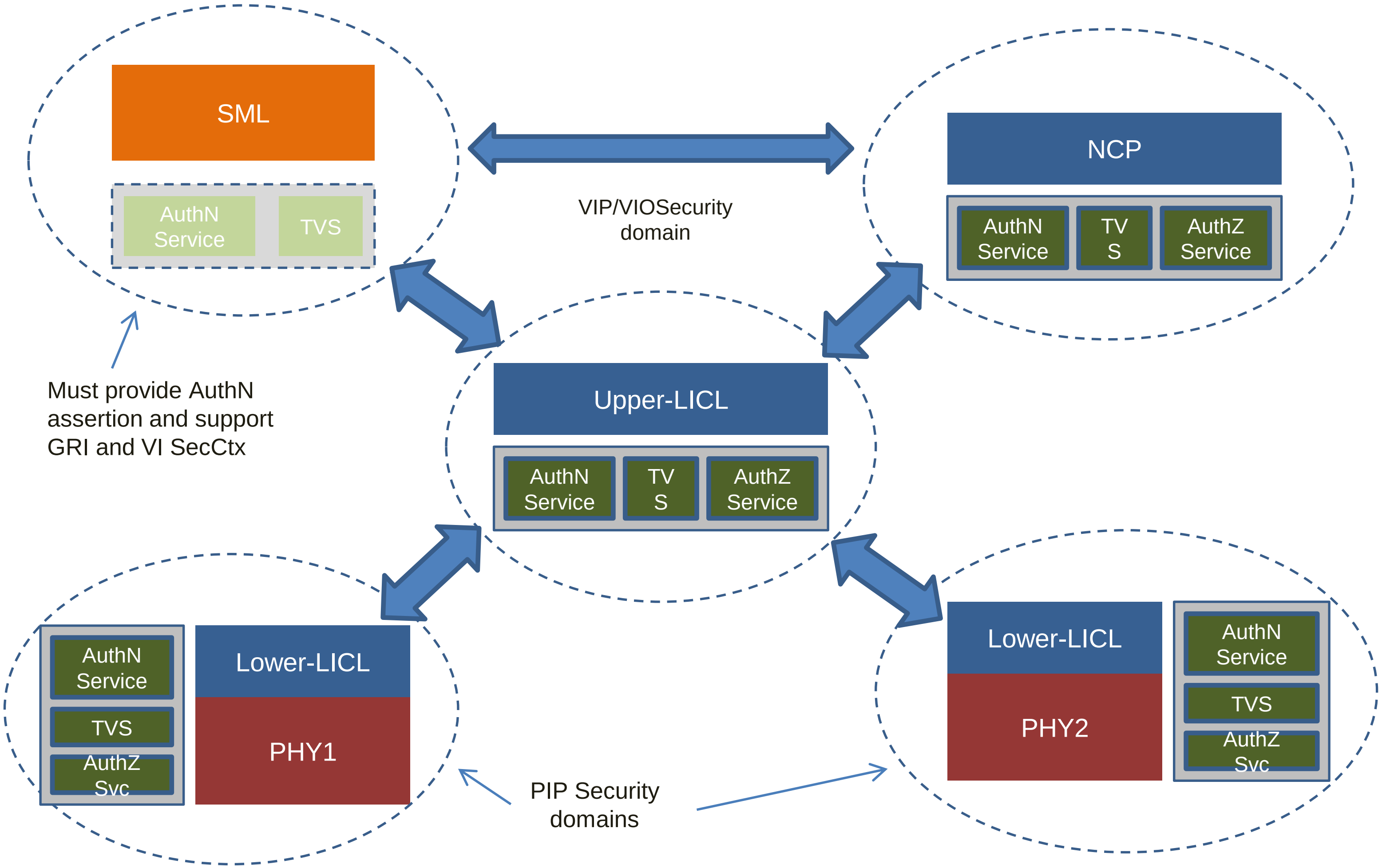
CSSI – Common Security Services Interface

# AAI Reference Model (GEYSERS)

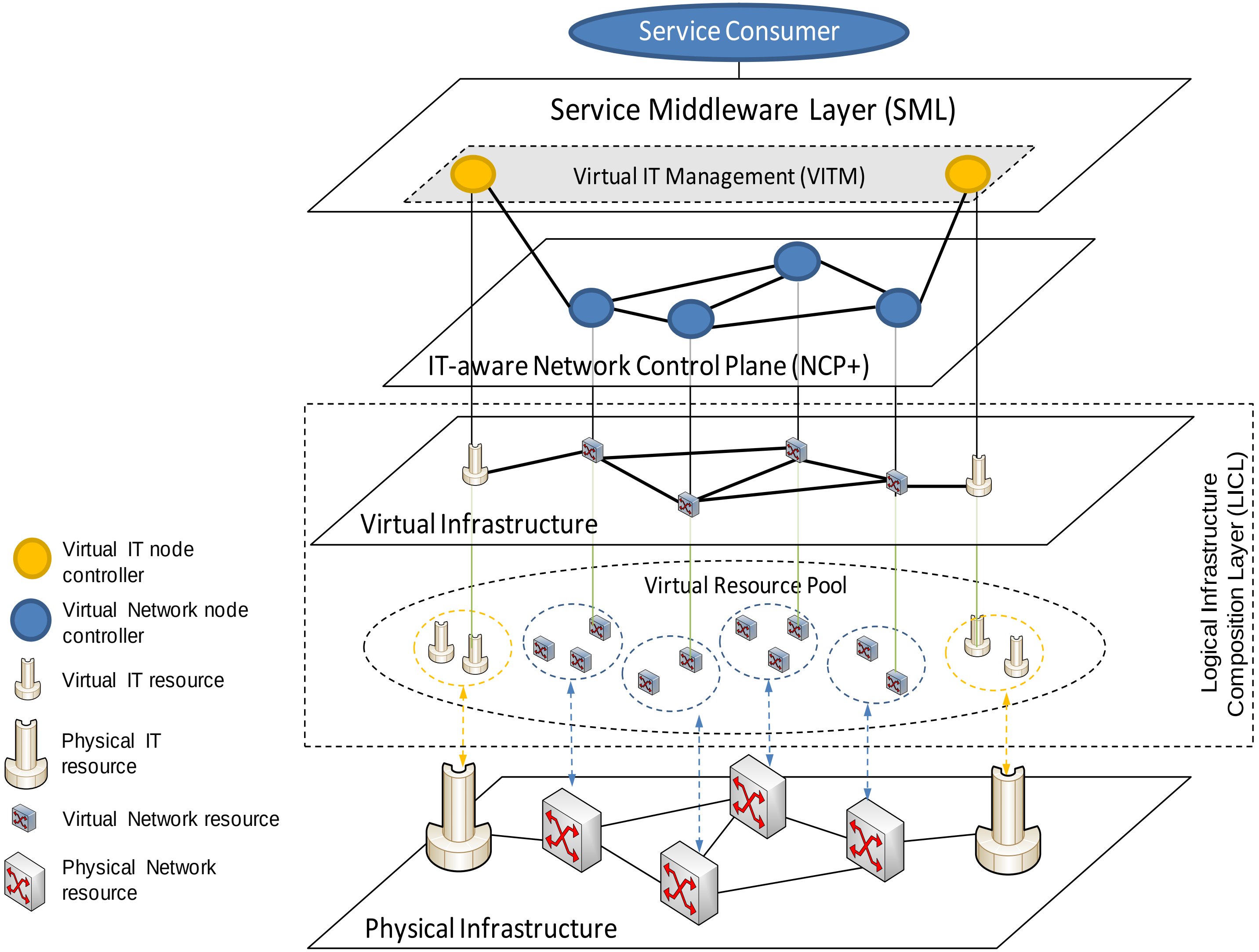


PEP: Policy Enforcement Point
PDP: Policy Decision Point
PAP: Policy Administration Point
DACS: Dynamic Access Control Service

# AAI in GEYSERS: Multi-domain and Multi-layer Environment



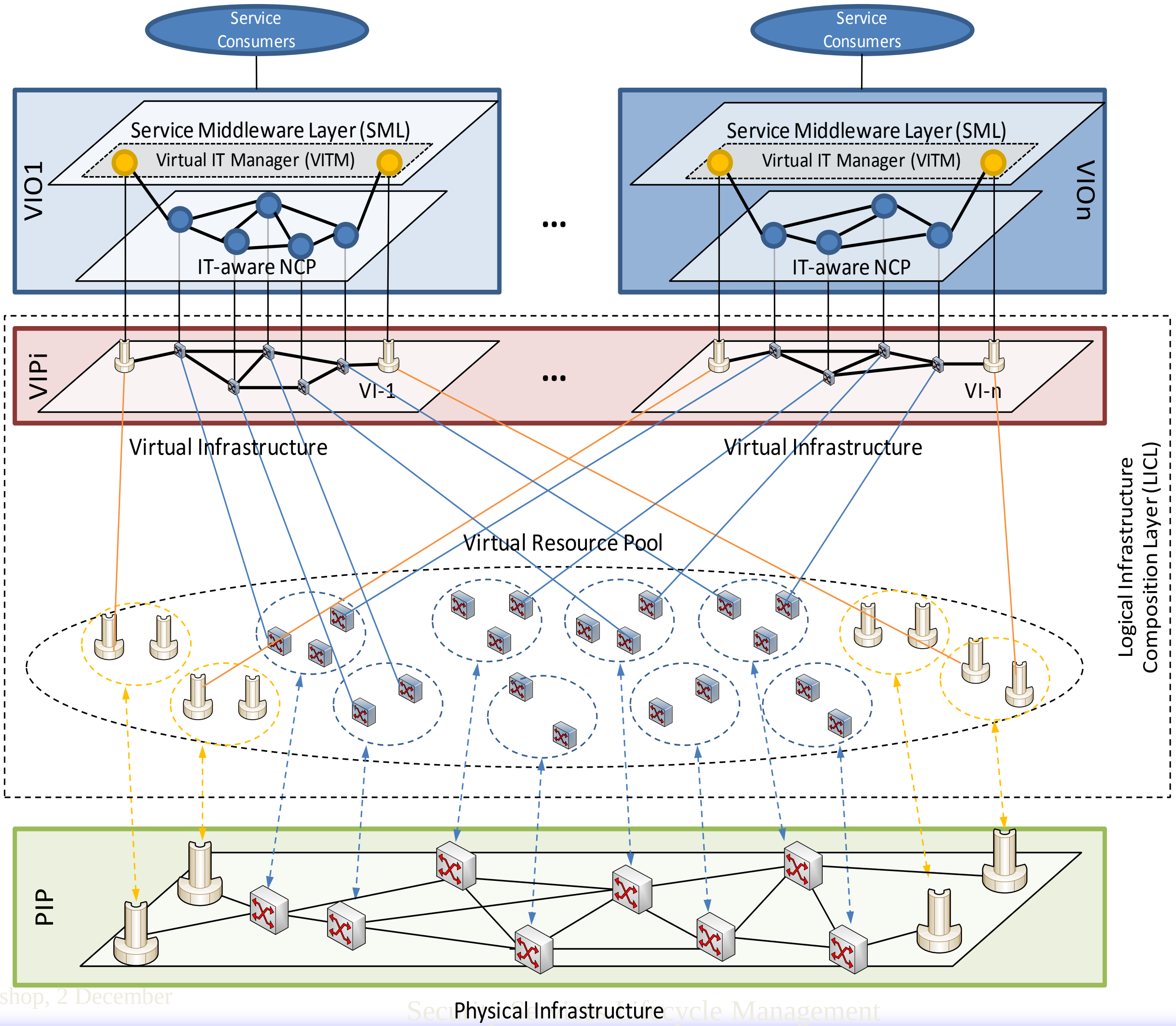
# GEYSERS Reference Model


Service Consumer
Service Middleware Layer (SML)
Virtual IT Management (VITM)
IT-aware Network Control Plane (NCP+)
Virtual Infrastructure
Virtual Resource Pool
Logical Infrastructure Composition Layer (LICL)
Physical Infrastructure
Virtual IT node controller
Virtual Network node controller
Virtual IT resource
Physical IT resource
Virtual Network resource
Physical Network resource

Roles/Actors

- VIO
- VIP
- PIP

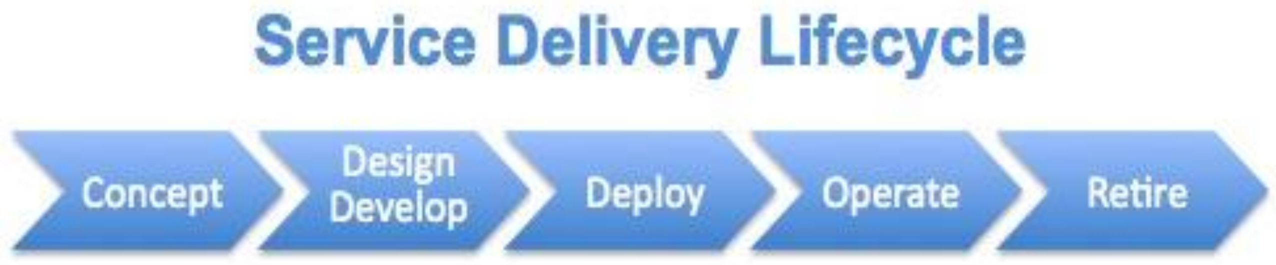
# Role of GEYSERS actors with respect to its architectural layers



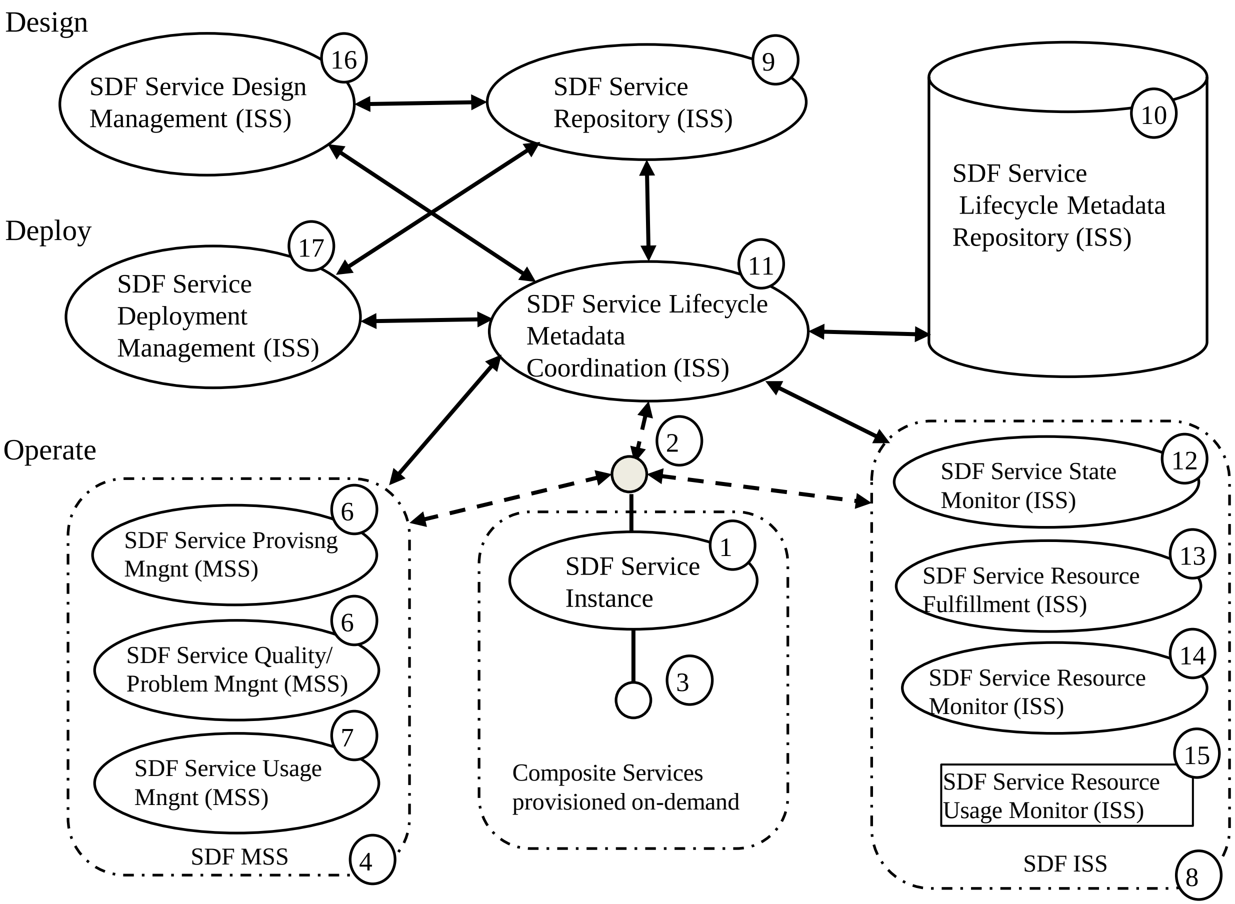
# TMF Service Delivery Framework (SDF)

Main goal – automation of the whole service delivery and operation process (TMF, http://www.tmforum.org/), 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



# SDF Reference Architecture (refactored from TMF SDF)


Design
SDF Service Design Management (ISS)
16
SDF Service Repository (ISS)
9
SDF Service Lifecycle Metadata Repository (ISS)
10
Deploy
SDF Service Deployment Management (ISS)
17
SDF Service Lifecycle Metadata Coordination (ISS)
11
Operate
2
SDF Service Provisng Mngnt (MSS)
6
SDF Service Quality/ Problem Mngnt (MSS)
6
SDF Service Usage Mngnt (MSS)
7
SDF MSS
4
SDF Service Instance
1
3
Composite Services provisioned on-demand
SDF Service State Monitor (ISS)
12
SDF Service Resource Fulfillment (ISS)
13
SDF Service Resource Monitor (ISS)
14
SDF Service Resource Usage Monitor (ISS)
15
SDF ISS
8

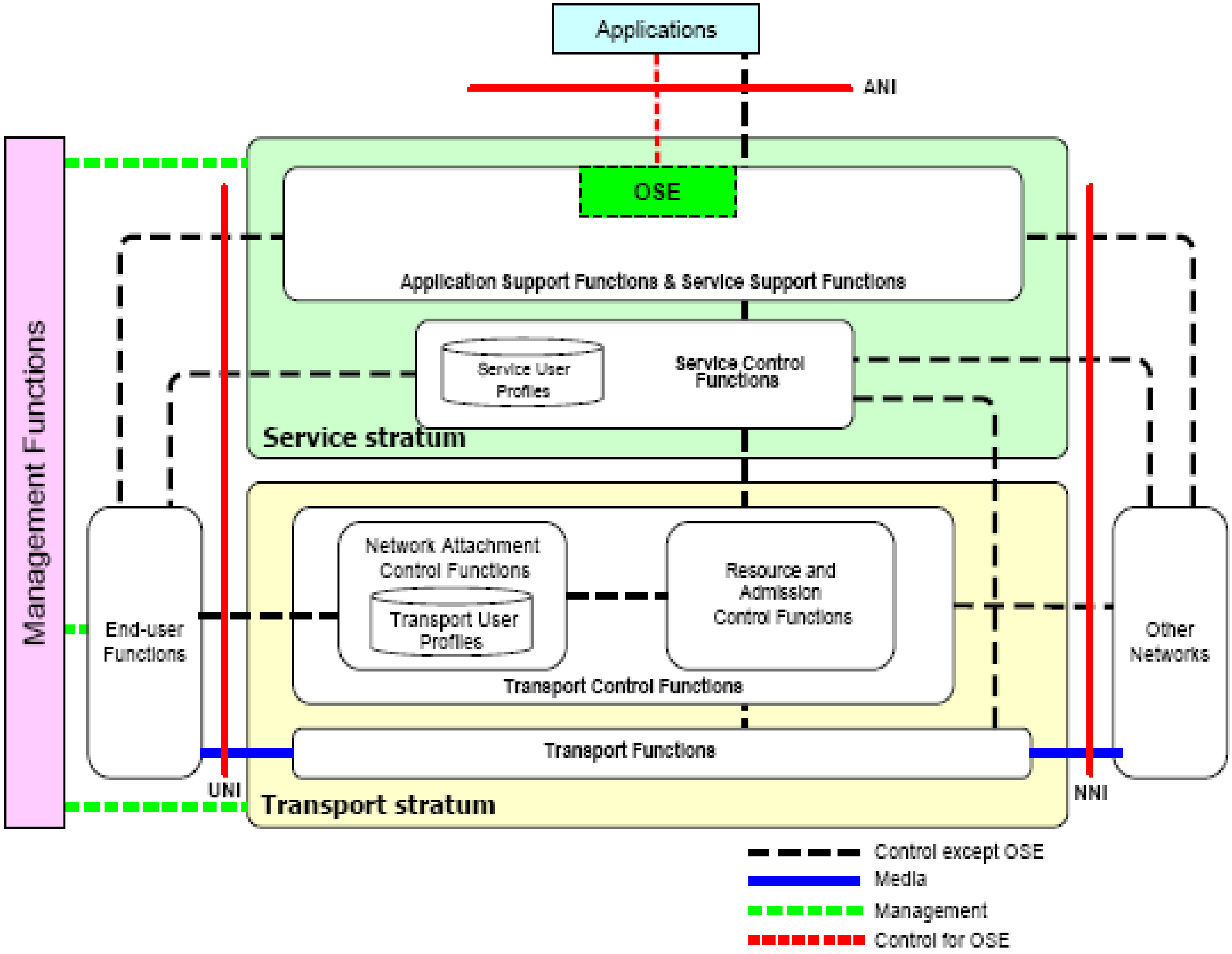
1 – Service Instance
2 - Service Management Interface
3 – Service Functional Interface
4 - Management Support Service (SDF MSS)
8 - Infrastructure Support Service (ISS)
DESIGN stage
9 - Service Repository
10 - Service Lifecycle Metadata Repository
16 - Service Design Management
DEPLOYMENT stage
10 - 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

# ITU-T NGN Open Service Environment

- **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 its interfaces (e.g., UNI, NNI, ANI) by applying X.805
  - Uses trust model based on NE supporting the functional Y.2012 entities
- ITU-T REC Y.2012 (09/2006) Functional requirements and architecture of the NGN release 1
- ITU-T REC Y.2011 (10/2004) General principles and general reference model for Next Generation Networks
- ITU-T REC Y.110 (06/98) Global Information Infrastructure principles and framework architecture
- ITU-T REC Y.2201 (04/2007) NGN release 1 requirements

.

# T-REC-Y.2234-200809 Open service environment capabilities for NGN (1)



- Extended NGN architecture positioning the OSE