Defining Generic Architecture
for
Cloud Infrastructure as a Service (IaaS) Provisioning Model

Yuri Demchenko, Cees de Laat
SNE Group, University of Amsterdam

ISGC2011 Conference
22-25 March 2011, Taipei

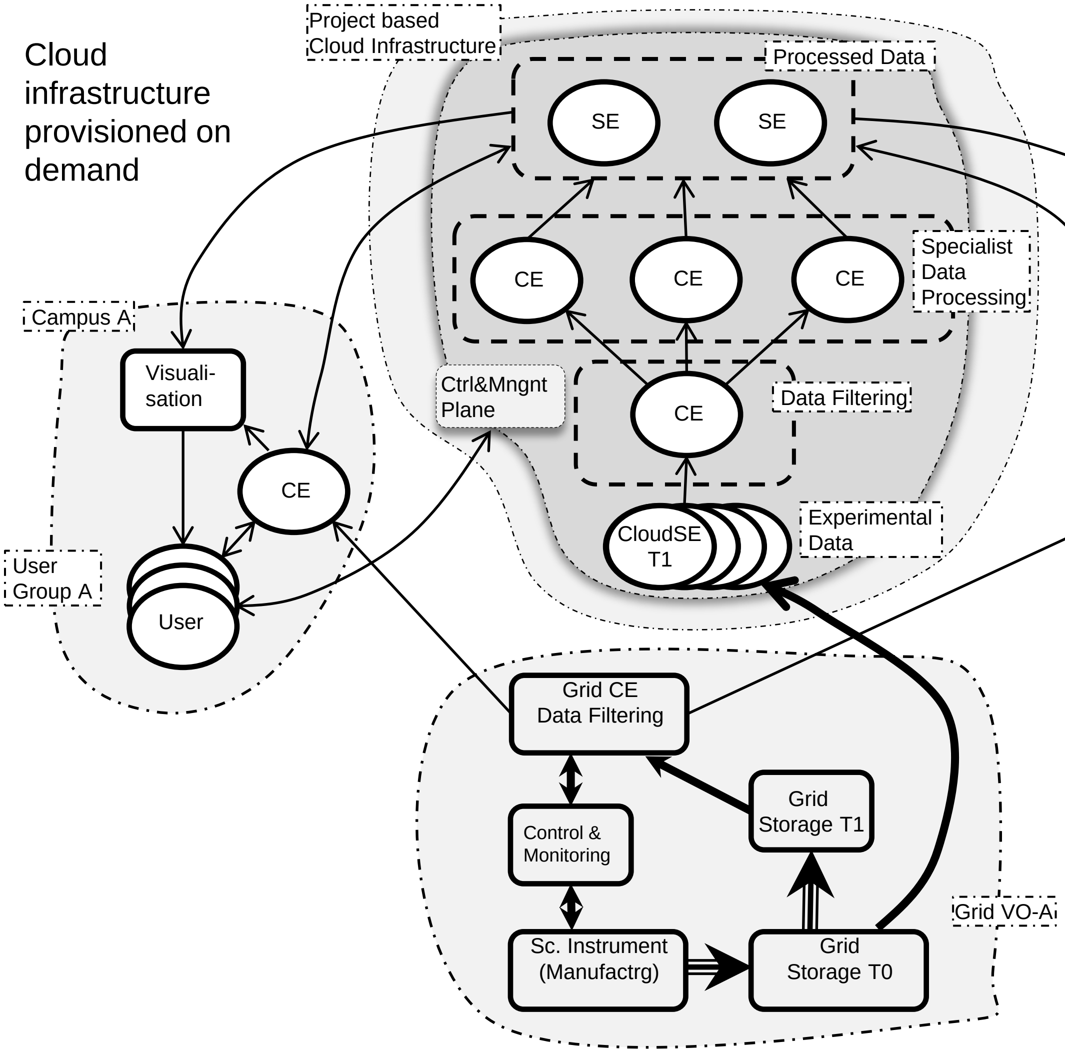
Outline

- System and Network Engineering (SNE) Group at the University of Amsterdam
- Basic use case from e-Science
- Proposed architectural framework
  - Infrastructure Services Modeling Framework (ISMF)
  - Composable Services Architecture (CSA)
  - Service Delivery Framework (SDF)
- Security aspects in Cloud computing
  - Security Services Lifecycle Management (SSLM) model

System and Network Engineering (SNE) 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 and infrastructure services description
  - 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, Cloud experiments 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 architectural framework for Cloud IaaS
  - Extending it for infrastructure security services and related security and trust models

Use case for Infrastructure Services Provisioning



Cloud infrastructure provisioned on demand

Project based Collaborating user groups located in remote campuses on data intensive projects requiring high performance computing and rich visualisation

Campus infrastructure including visualisation tools

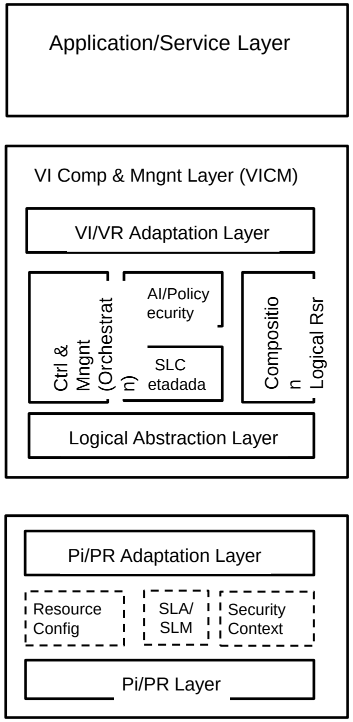
Grid based core eScience Infrastructure including data intensive scientific instrument

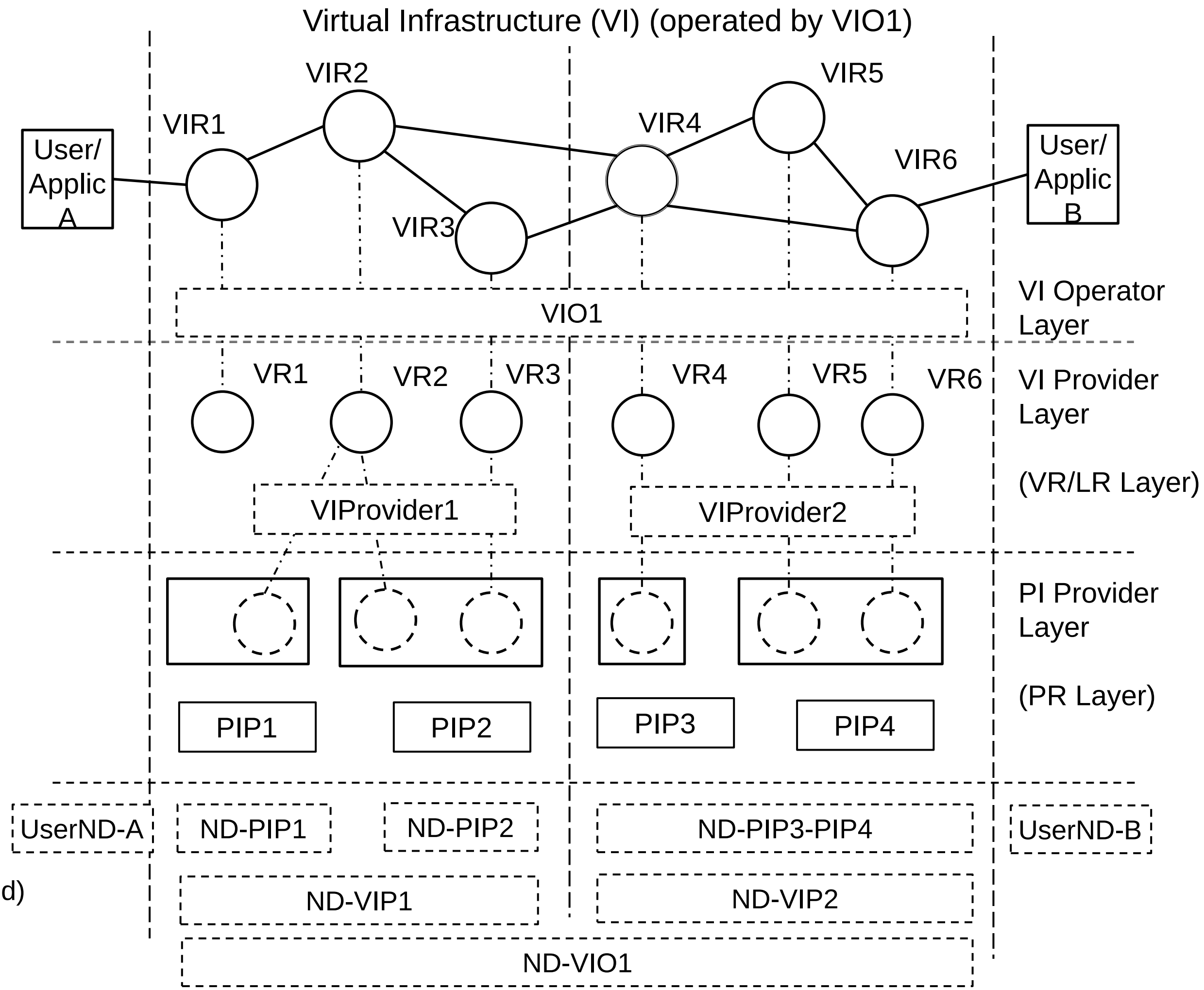
Proposed Architectural Framework for Cloud IaaS

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

- **Infrastructure Services Modeling Framework (ISMF)** that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring
- **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
- (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 Abstract Model



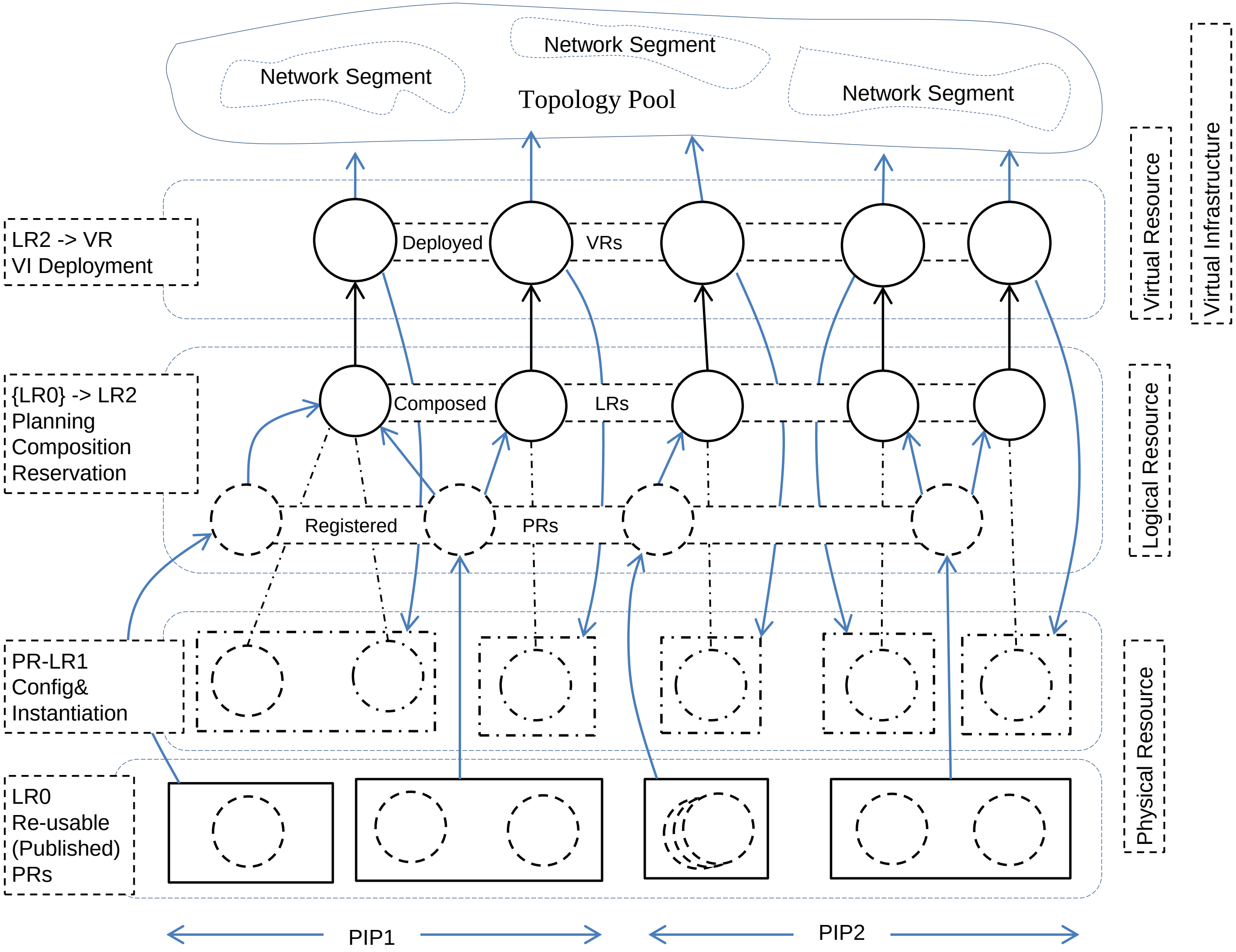


Legend
ND* - Network Domain
VIR* - VI Resource (deployed)
VR – Virtual Resource
LR – Logical Resource
PR – Physical Resource

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 SDF 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



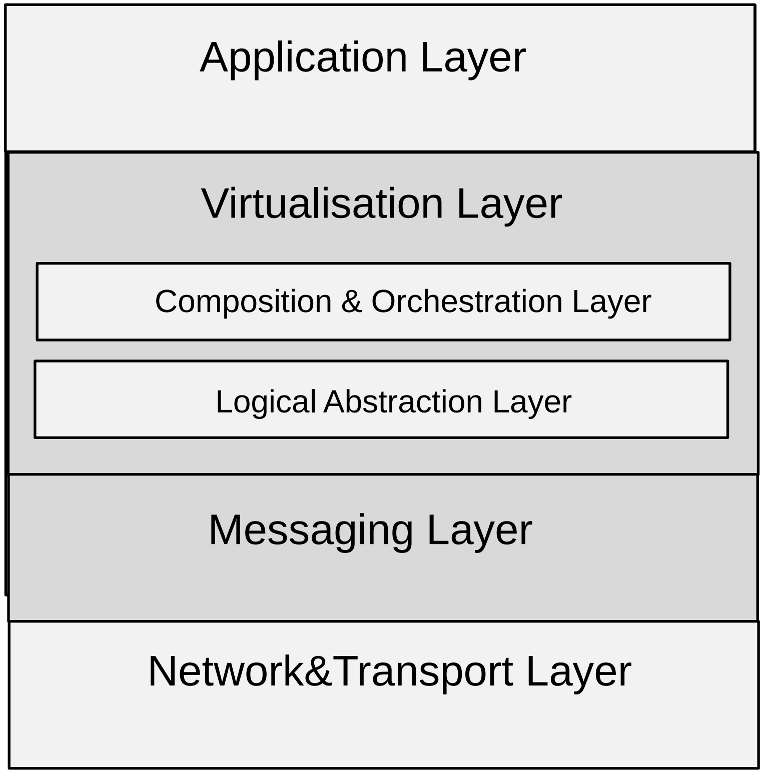
ISMF - Relation between PR-LR-VR-VI

- 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

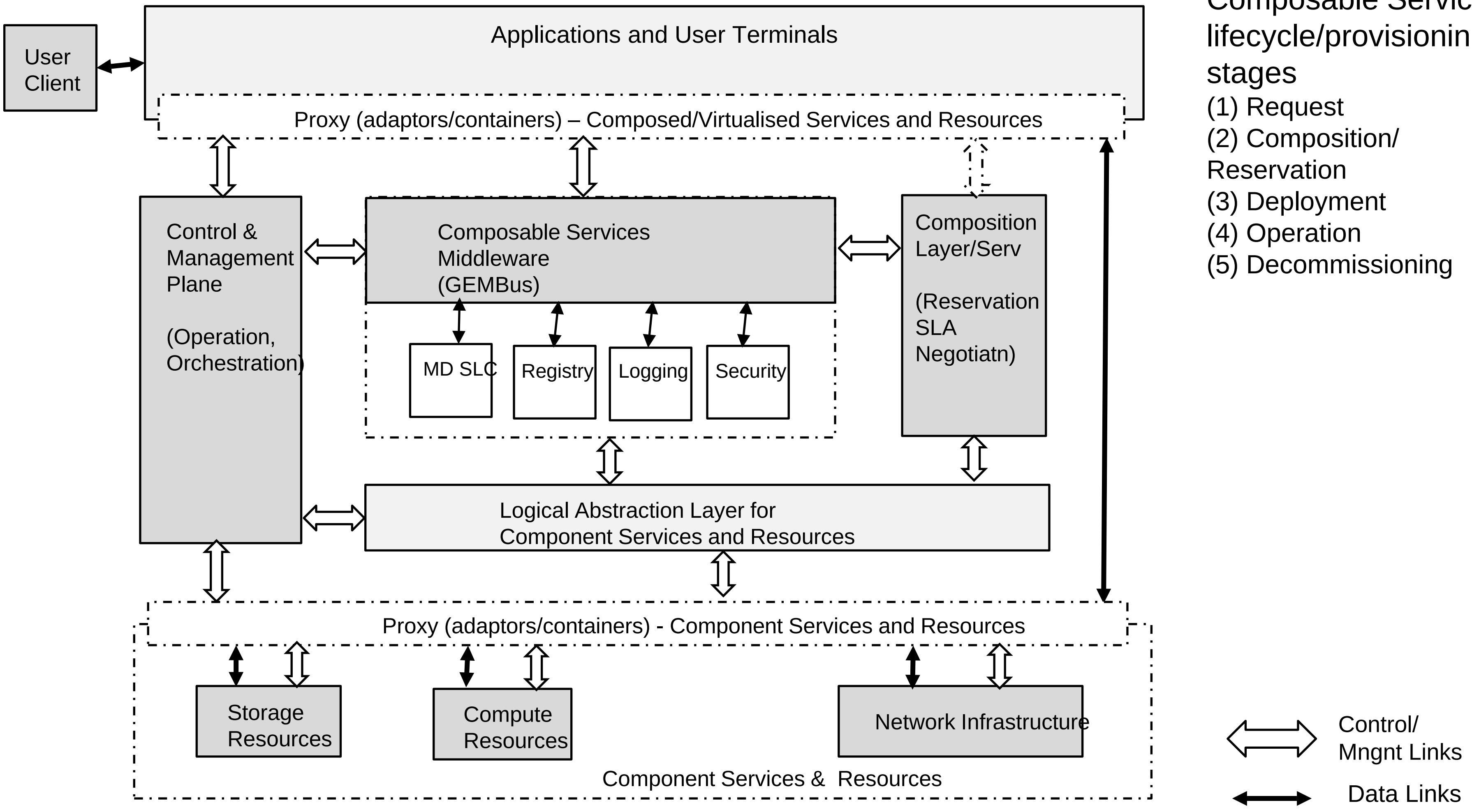
Messaging Layer

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

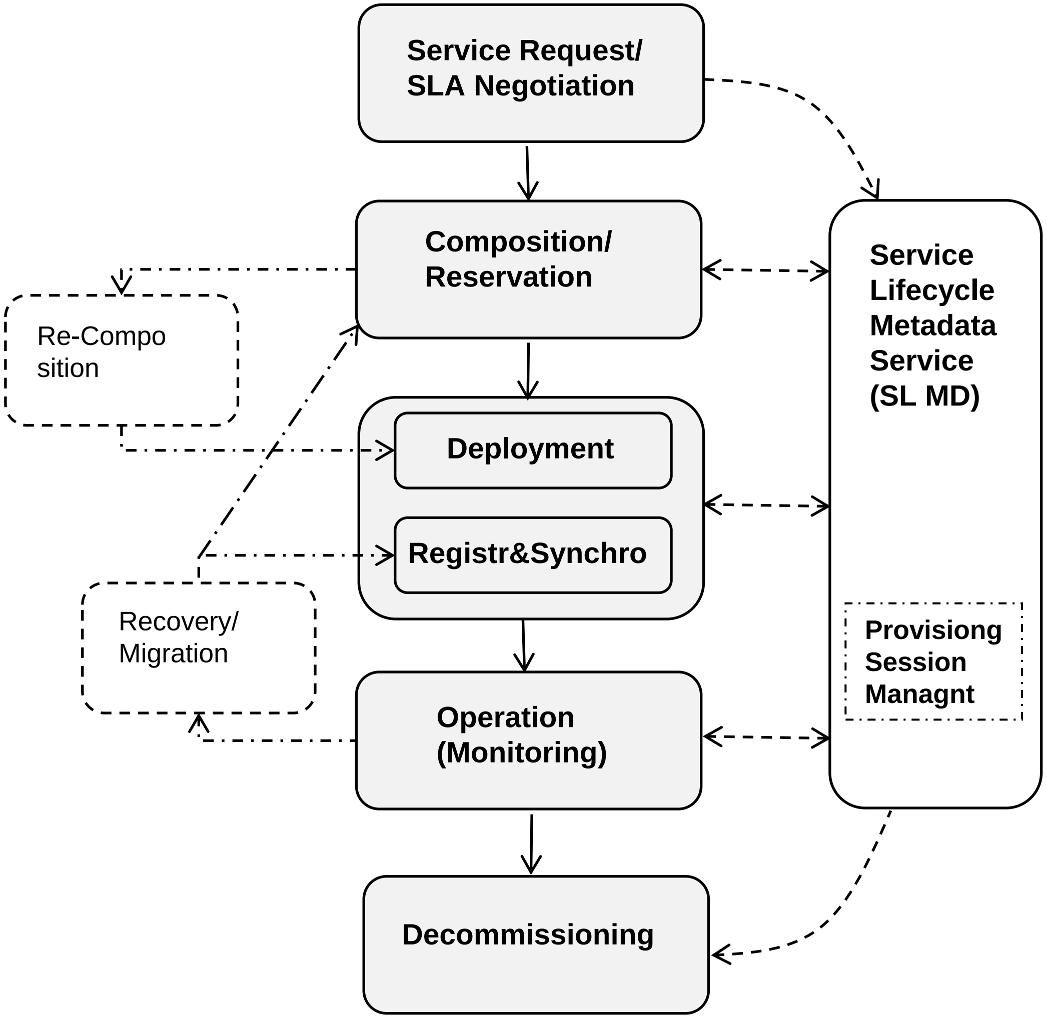
Composable Services Architecture – Version 0.13


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
Control/ Mngnt Links
Data Links

Composable Services lifecycle/provisioning stages

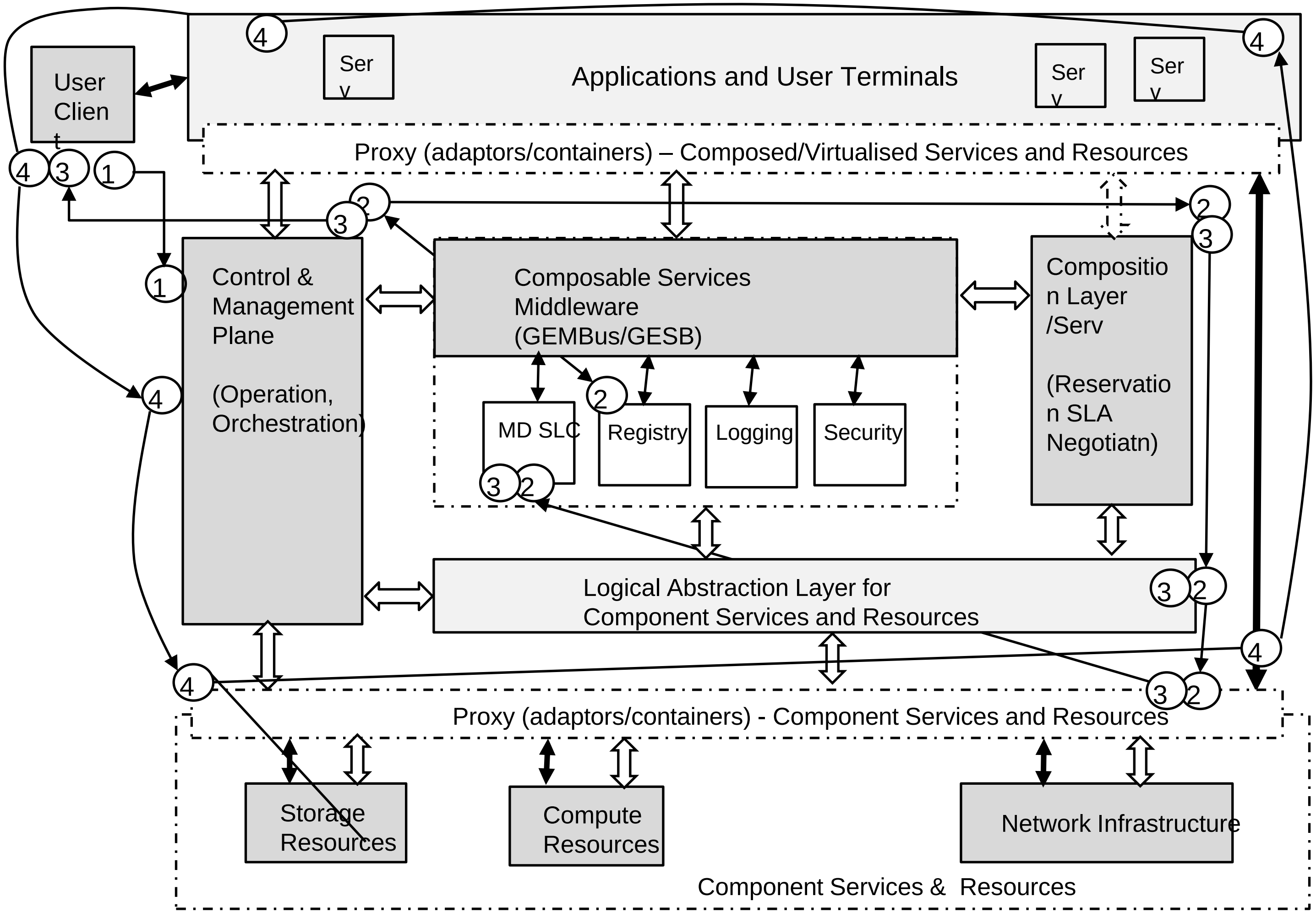
(1) Request
(2) Composition/ Reservation
(3) Deployment
(4) Operation
(5) Decommissioning

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


Applications and User Terminals
Ser v
Ser v
Ser v
User Clien t
4
3
1
4
4
Proxy (adaptors/containers) – Composed/Virtualised Services and Resources
2
3
2
3
1
Control & Management Plane
(Operation, Orchestration)
Composable Services Middleware (GEMBus/GESB)
Compositio n Layer /Serv
(Reservatio n SLA Negotiatn)
4
MD SLC
Registry
Logging
Security
2
3
2
Logical Abstraction Layer for Component Services and Resources
3
2
4
4
3
2
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

MD SLC – Service Lifecycle Metadata

GEMBus – GEANT Multidomain Bus

GESB – Geysers ESB

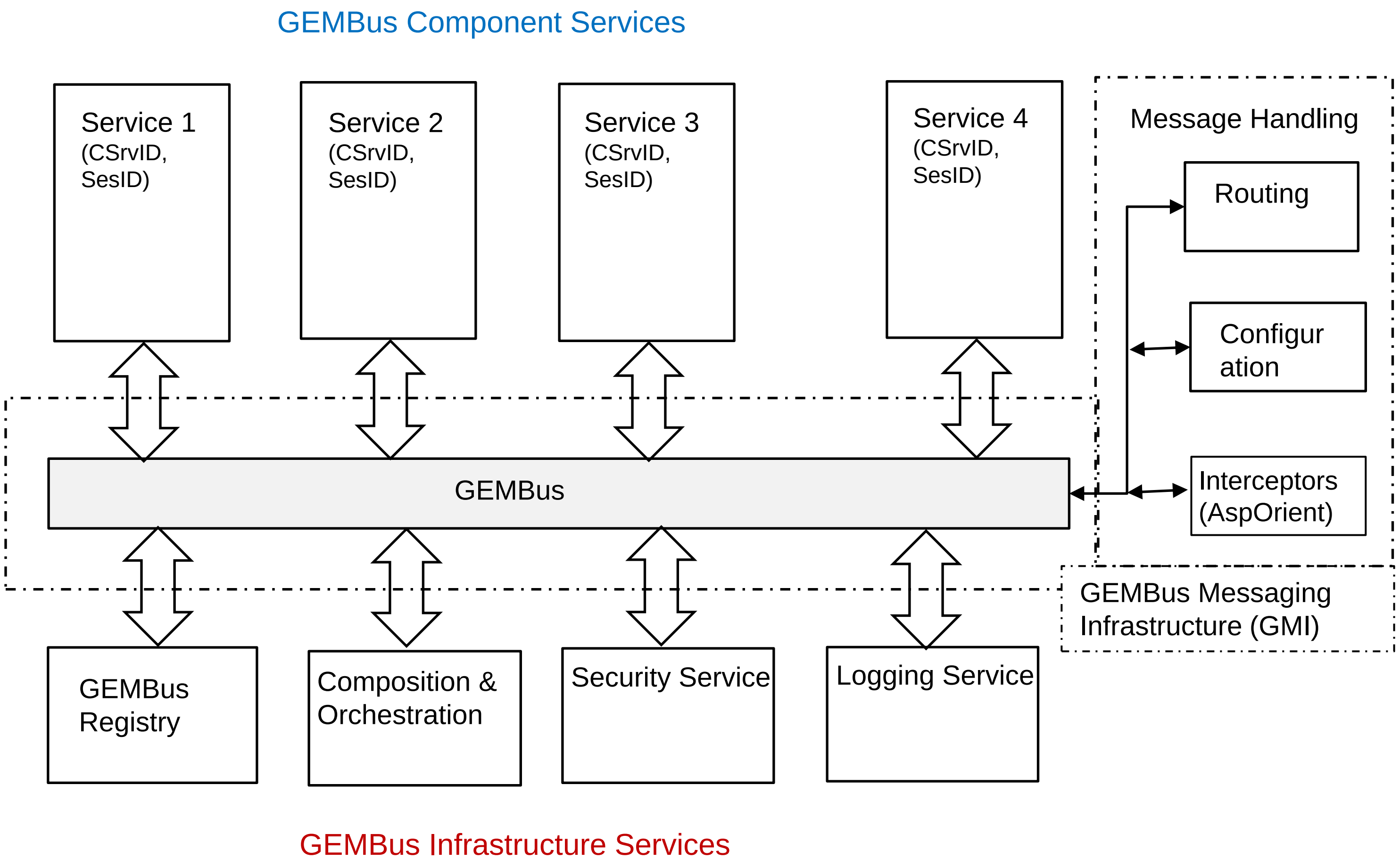
⇔ Control/ Mngnt Links

↔ Data Links

CSA functional elements interaction

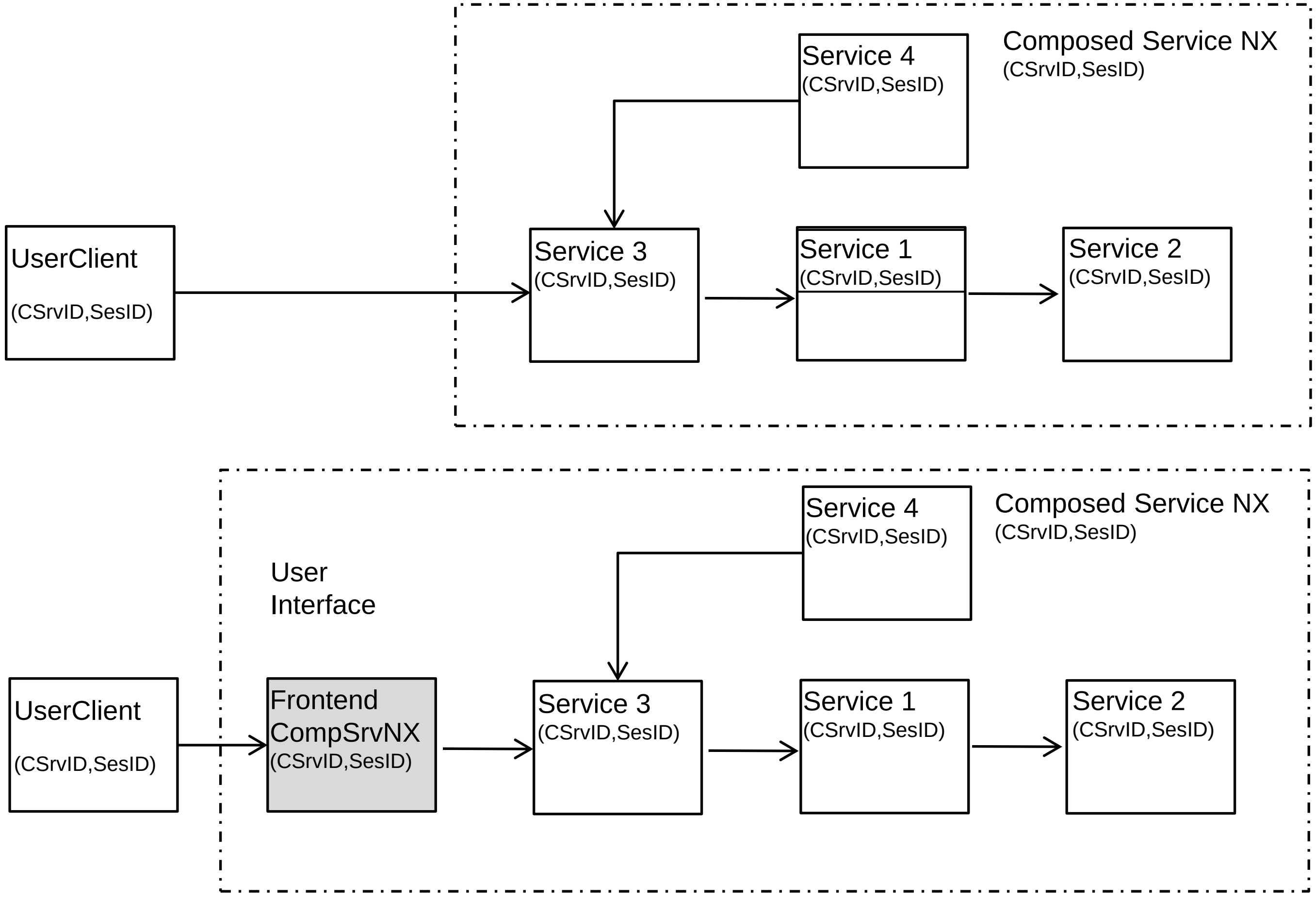
- **(1) Request**
  - User Client -> Control and Management
- **(2) Composition/ Reservation**
  - Control&Mngnt -> Registry -> Composition/Reservation Serv -> (Logical Abstract -> Resr Adapters) -> LC Metadata Serv
- **(3) Deployment**
  - Control&Mngnt -> Composition/Reservation Serv -> (Logical Abstract -> 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 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

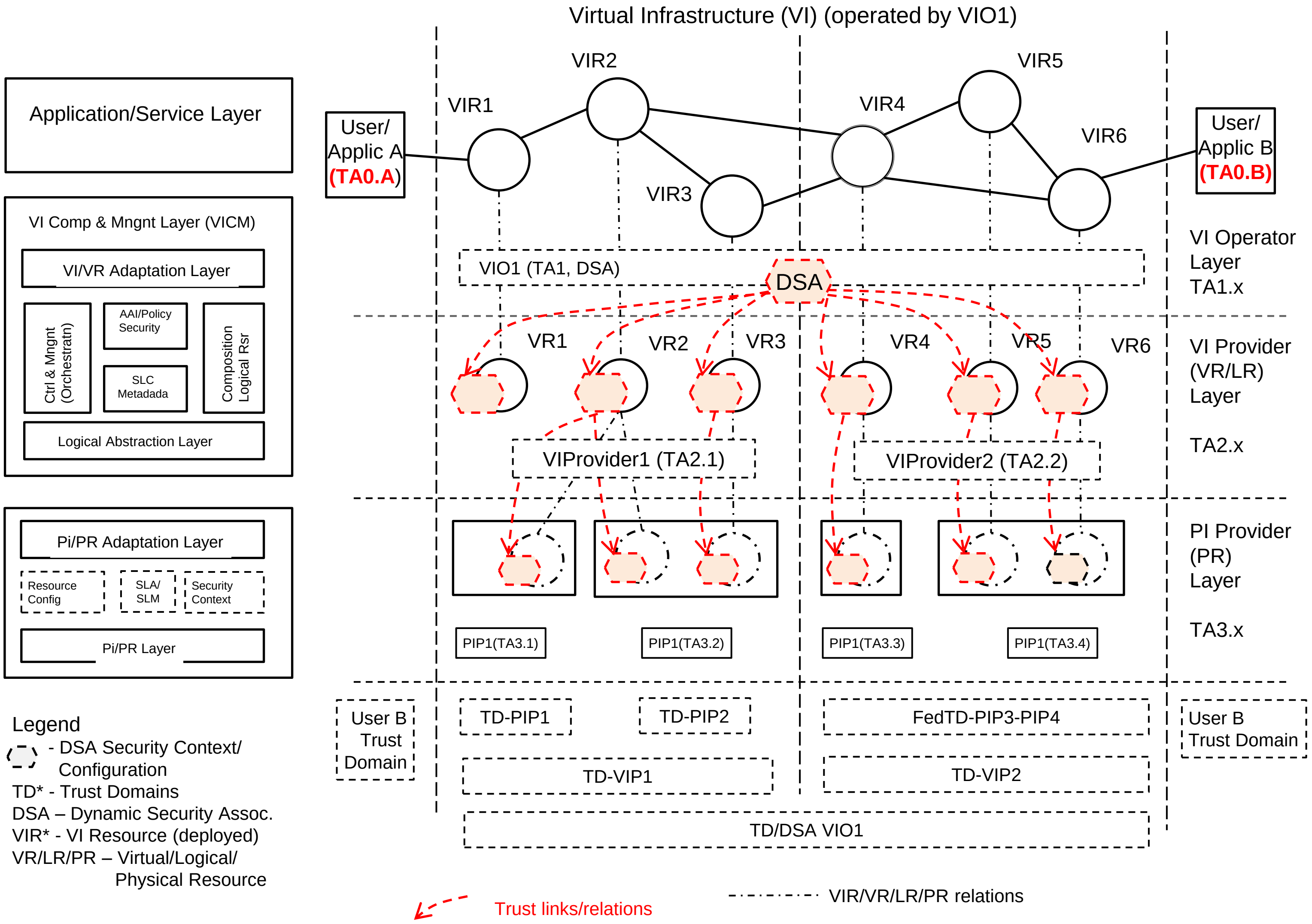
Cloud Security – Problem area and issues

- Virtualised services
- On-demand/dynamic provisioning
- Multi-tenant/multi-user
- Multi-domain
- Uncontrolled execution and data storage 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

Current Cloud Security Model

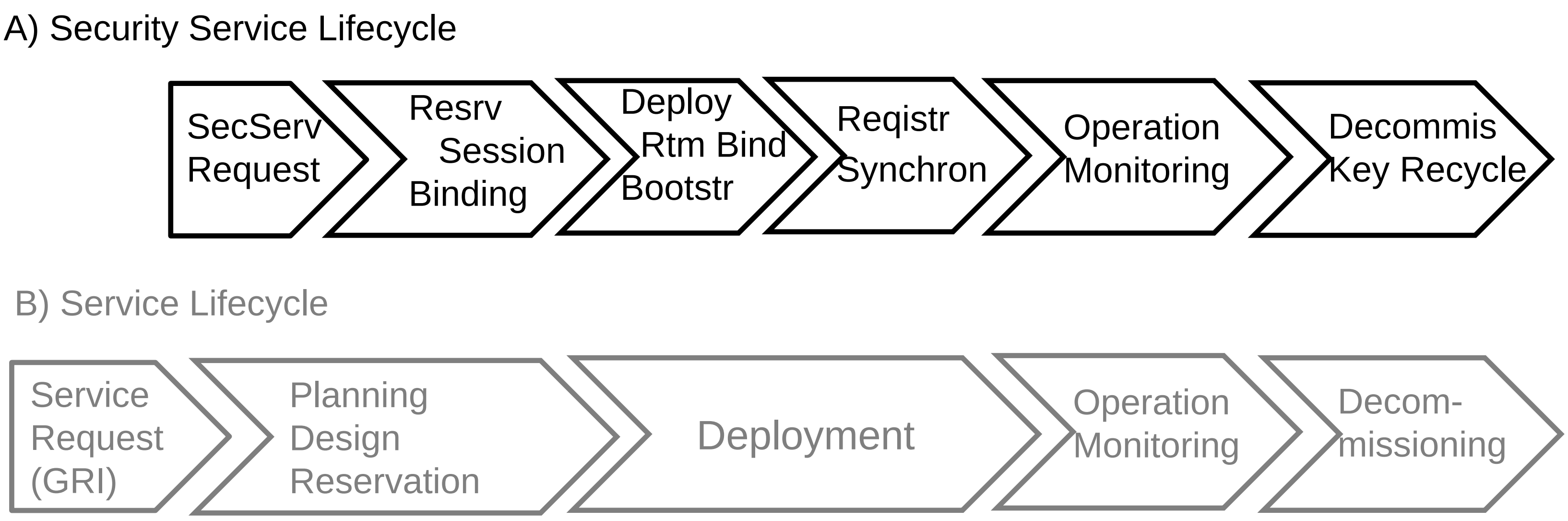
- SLA based security model
  - SLA between provider and user defines the provider responsibility and guarantee
  - Providers undergo certification
  - Standard business model
- Using VPN and SSH keys generated for user infrastructure/VMs
  - Works for single Cloud provider
- Has inherited key management problems
- Not easy integration with legacy physical resources
- Not scalable
- Simple access control, however can be installed by user
- Trade-off between simplicity and manageability

Security Infrastructure for IaaS



Legend
- DSA Security Context/ Configuration
TD* - Trust Domains
DSA – Dynamic Security Assoc.
VIR* - VI Resource (deployed)
VR/LR/PR – Virtual/Logical/ Physical Resource

Security Services Lifecycle Management Model



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.

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**

Future developments

- Further development of the proposed architectural components in GEANT3 and GEYSERS projects
  - Demo at SuperComputing 2011 Conference and exhibition
- Dynamically provisioned security infrastructure
  - Dynamic security association
- Contribution to OGF ISOD-RG activity
- EU wide cooperation and possible EU project

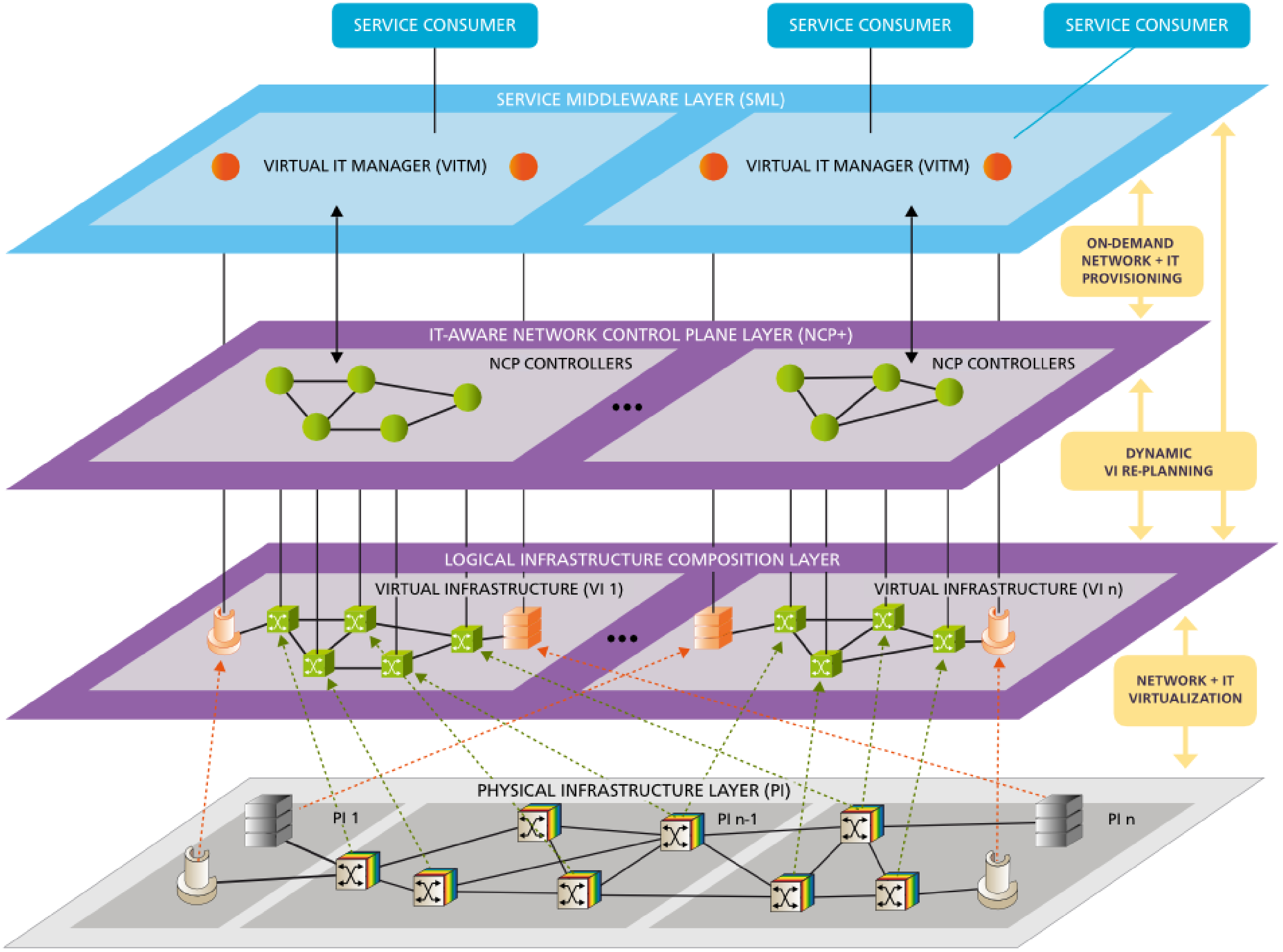
Acknowledgement

•This work is supported by the FP7 EU funded project GEANT3 (FP7-ICT-238875), and the FP7 EU funded Integrated project The Generalised Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657).

Additional Information

- GEYSERS project reference architecture

GEYSERS Reference Architecture


SERVICE CONSUMER
SERVICE CONSUMER
SERVICE CONSUMER
SERVICE MIDDLEWARE LAYER (SML)
VIRTUAL IT MANAGER (VITM)
VIRTUAL IT MANAGER (VITM)
ON-DEMAND NETWORK + IT PROVISIONING
IT-AWARE NETWORK CONTROL PLANE LAYER (NCP+)
NCP CONTROLLERS
...
NCP CONTROLLERS
DYNAMIC VI RE-PLANNING
LOGICAL INFRASTRUCTURE COMPOSITION LAYER
VIRTUAL INFRASTRUCTURE (VI 1)
...
VIRTUAL INFRASTRUCTURE (VI n)
NETWORK + IT VIRTUALIZATION
PHYSICAL INFRASTRUCTURE LAYER (PI)
PI 1
PI n-1
PI n

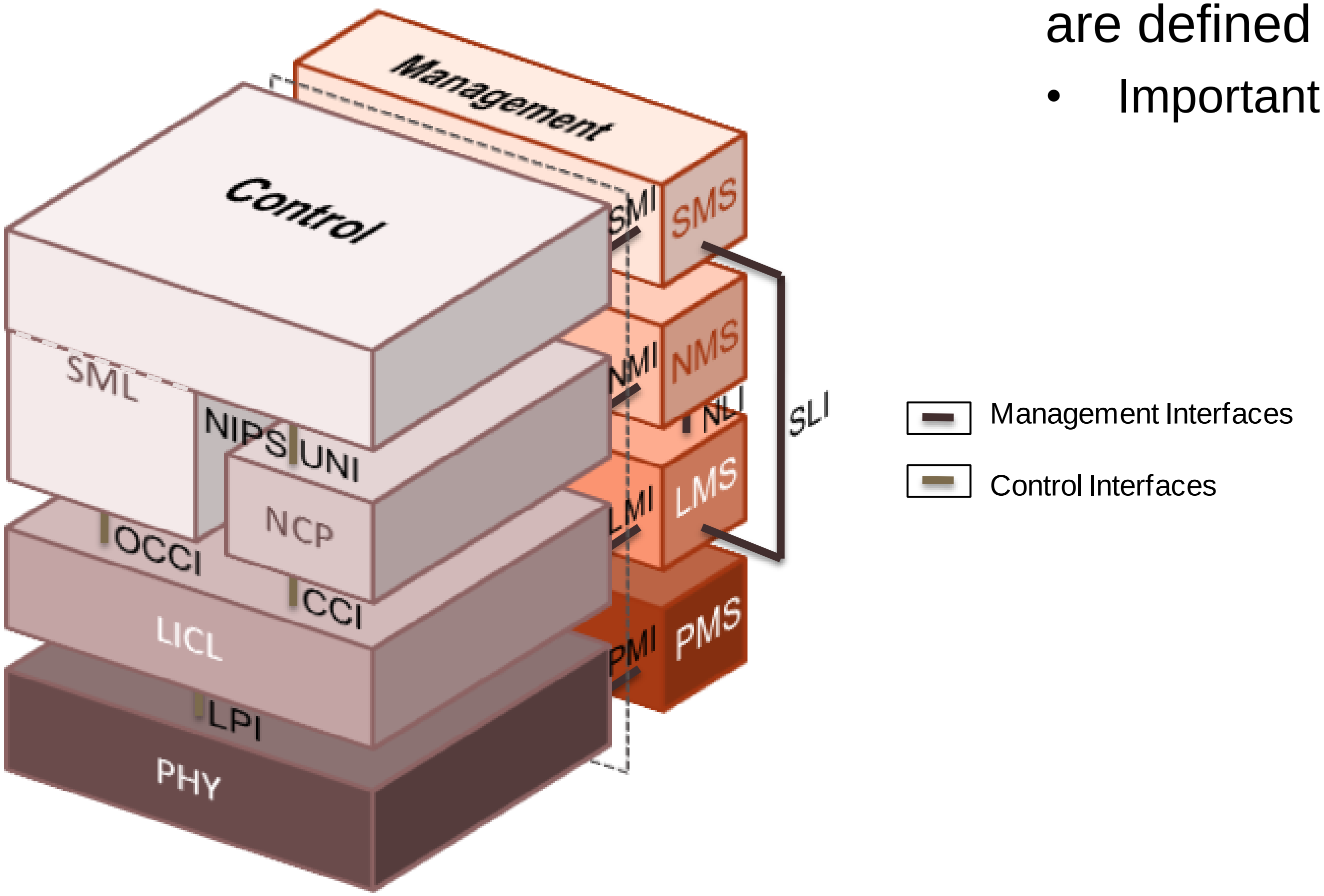
SC
(Service Consumer)

VIO
(Virtual Infrastructure Operator)

VIP
(Virtual Infrastructure Provider)

PIP
(Physical Infrastructure Provider)

GEYSERS Layered Architecture



Control and Management Planes are defined

- Important for consistent design

General security services/aspects

- ✓ 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 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.

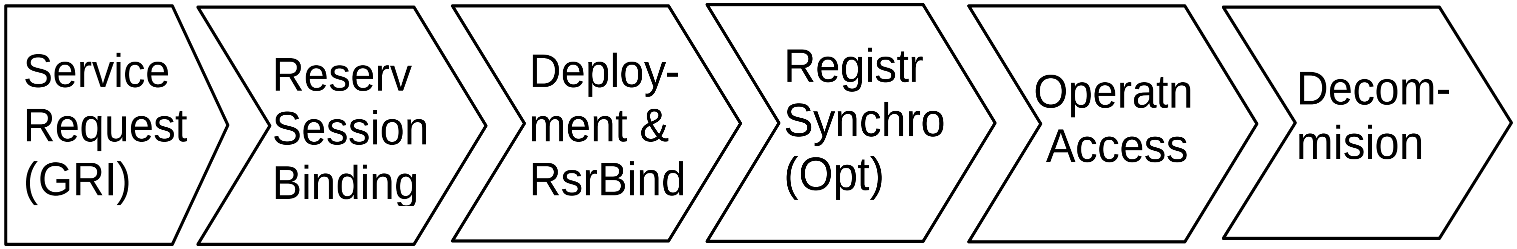
- **Reservation session binding** that provides support for complex reservation process including required access control and policy enforcement.

- **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.



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
- Defining architecture for dynamically configured security services/infrastructure
- OGF On-Demand Infrastructure Service (ISOD) provisioning BoF/RG
  - Including definition of IaaS and required security models