On-Demand Infrastructure Services Provisioning in Geysers Project and Security Services Lifecycle Management

Yuri Demchenko
SNE Group, University of Amsterdam

SNE Group Meeting
11 February 2010, Amsterdam

Outline

- Geysers project overview
  - SNE/UvA contribution
- Security issues in on-demand services provisioning
- Standardisation in Service/Resource Operations and Delivery
  - ITU-T, TMF, IPsphere, OpenGroup
- Proposed Security Services Lifecycle Management Model
- Suggested further steps and developments

Generic AAA Authorisation framework for on-demand multidomain NRP – Projects and developments

- Generic AAA Authorisation framework (GAAA-AuthZ) was proposed in RFC 2902, RFC2904 (2000) and defined general functional modules and their interaction with network services to support policy based network access control
  - Currently being extended to multidomain heterogeneous Network Resource Provisioning (GAAA-NRP)
- Phosphorus Project
  - GAAA-NRP developed and implemented
  - NRP model and inter-domain secure sessions management
  - Reference implementation in the GAAA Toolkit (GAAA-TK) Java library
- GN3 JRA3 Task 3 Composable services
  - GEant Multi-domain Bus (GEMBus) Security/AAA issues and services delivery lifecycle/workflow
- GEYSERS Infrastructure virtualisation and provisioning
  - Pluggable/integrated security services as a component of the virtualised infrastructure services delivery

GEYSERS Project Overview

- Activity: ICT-2009.1.1 The Network of the Future call 4 FP7
- Grant agreement for: Project duration 36 months
- Project start date: January 2010
- Project budget: 10.433.205 euro (7.035.000 euro EC contr.)
- Project resources: 947 person months

GEYSERS – Infrastructure provider's view

"Today's telecom operators face the need for providing users with dynamic high capacity and high-performance optical networks connectivity services tightly bounded with IT resources"

Applications provider view -

Google Fiber for Communities Project

http://www.google.com/appserve/fiberrfi/public/overview

- Next generation applications
- New deployment techniques

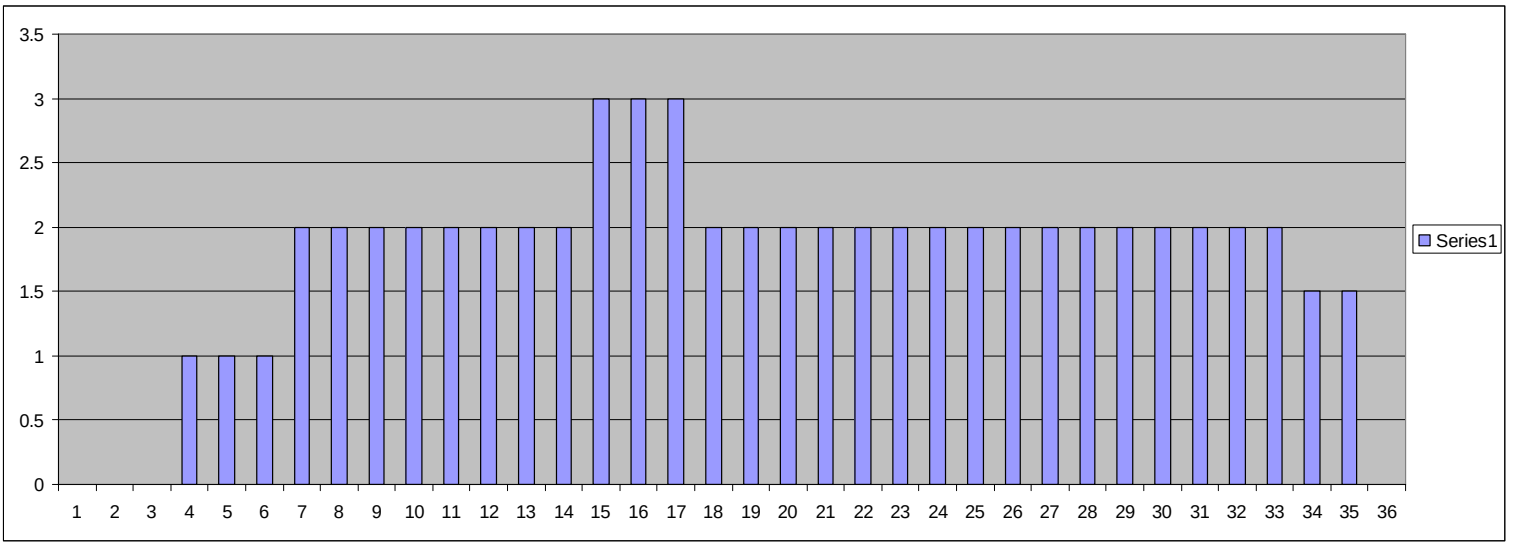
GEYSERS Project Structure - Workpackages

- WP1 – Business Models Analysis and Service Requirements
- WP2 – GEYSER Service Architecture and Interfaces Specifications
- WP3 – GEYSER Logical Infrastructure Composition Layer (LICL)
  - T3.1 Functional Logical Infrastructure Composition Layer (LICL) definition and design (leader i2CAT)
  - **T3.2 Information Modelling Framework (leader UvA)**
  - T3.3 Resource Synchronization (leader INRIA)
  - T3.4 Abstraction and Composition of Resources (leader I2CAT)
  - T3.5 System Integration (leader i2CAT)
- WP4 – GEYSER Network Control Plane (NCP) and Application Signalling Framework (ASF)
  - ***T4.2: Network+IT Provisioning Service (NIPS) user-network interface and procedures***
  - ***T4.3: NCP software architecture and high level design***
- WP5 – Integration, Validation and Demonstration
- WP6 – Exploitation/Dissemination and Standardization

SNE/UvA Contribution in GEYSERS

Two main areas

- Logical Layer Infrastructure Description Language (re-factoring NDL/NML)
  - WP2, WP3
- Dynamically configured composable Security services
  - WP2, WP3, WP4



UvA's MM distribution

Everage – 2 FTE starting from M4

GEYSERS VISION I

- **A novel architecture** capable of
  - Seamless and **coordinated provisioning** of optical network plus IT resources
  - **End-to-end service delivery** that overcomes limitations of network/domain segmentation

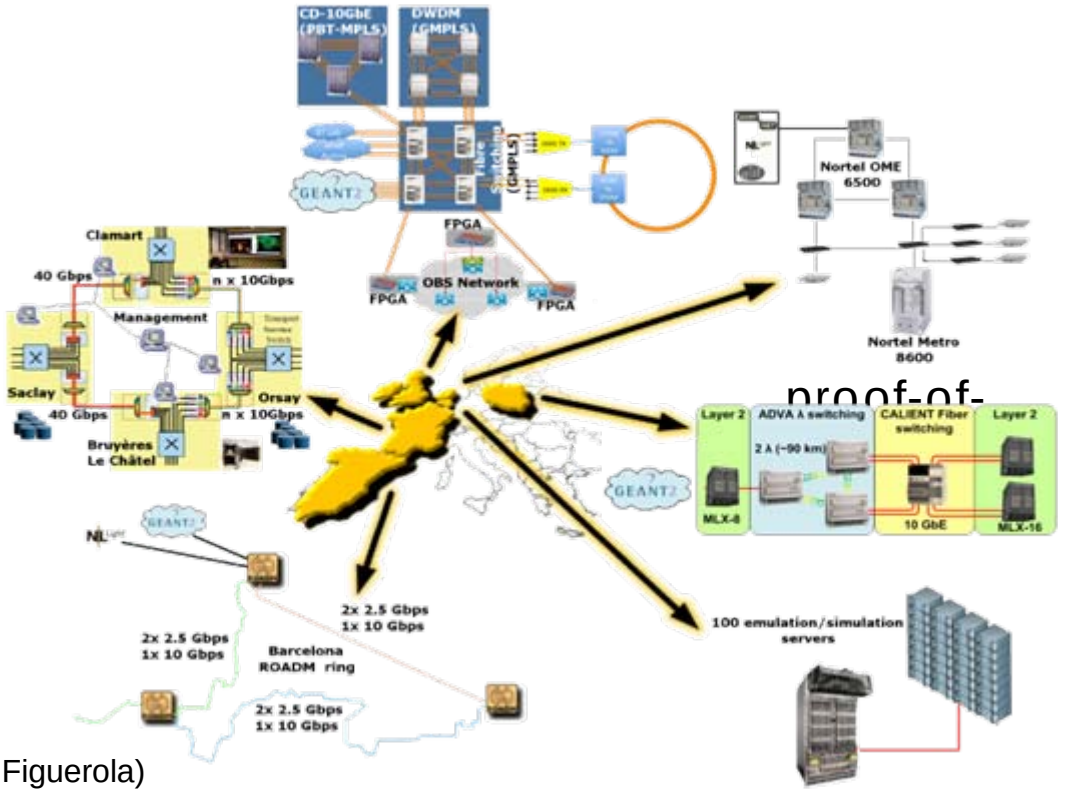
- A novel **business framework** for network infrastructure provider and network operators (service providers).

- Novel mechanism for infrastructure providers to partition infrastructure resources to compose **logical infrastructures** and offer them to network operators **as a service** (IaaS)

Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

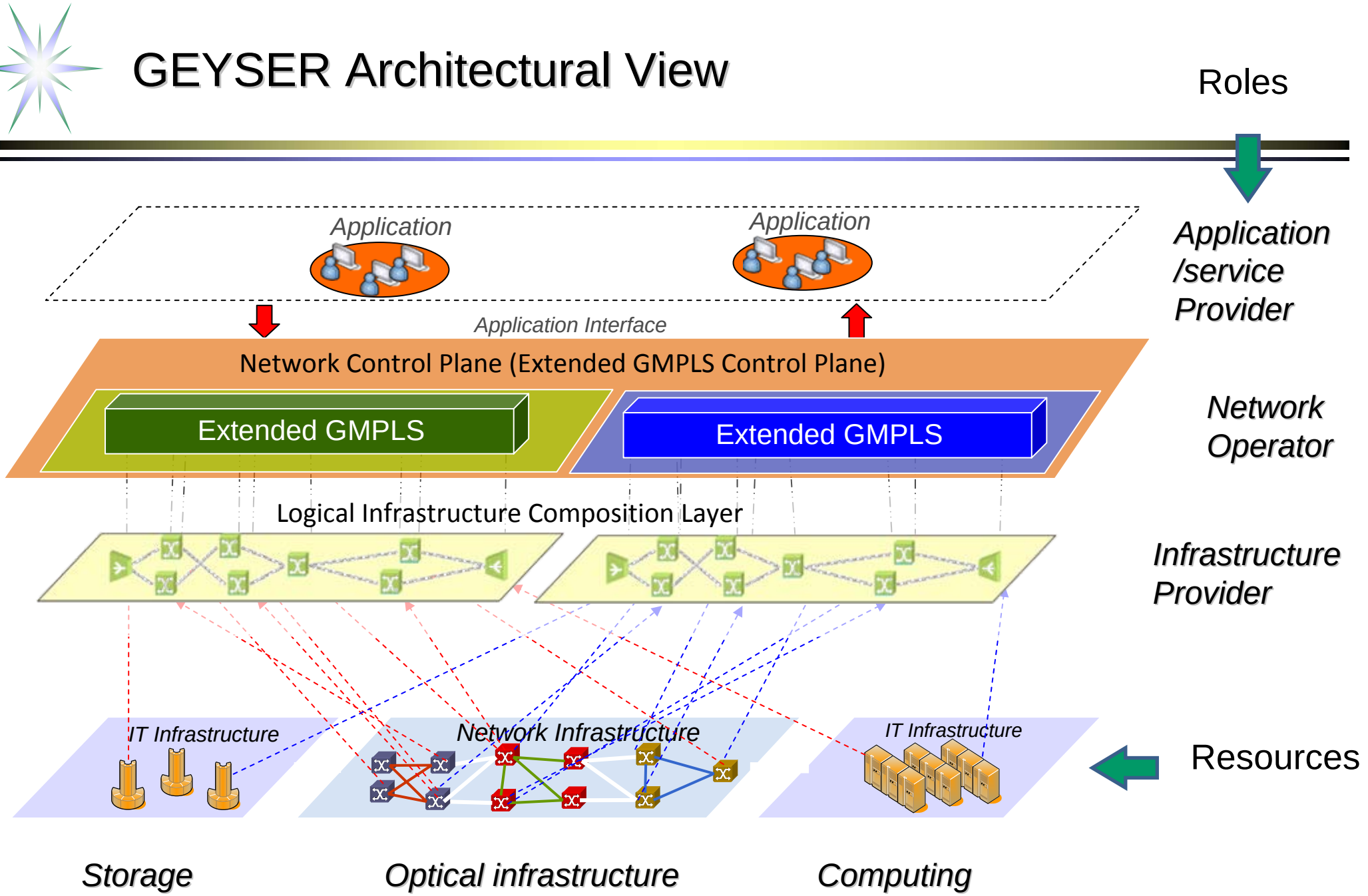
GEYSERS VISION II

- Enhanced GMPLS/PCE control plane for **dynamic control and re-planning of infrastructure resources** (Net + Any IT) based on End Users and Network Operator requirement.
- Customizable **SLAs for** vertical and horizontal requirements **deployment, trust, security and access control.**
- A distributed and multi-site **validation test-bed**
- A **cost & energy-efficient**, proof-of-concept implementation



Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

GEYSER Architectural View



Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

GEYSER Technical Innovations and Impact

- Main areas of innovation:
  - Logical Infrastructure composition and management
  - IT and Transport service provisioning

Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

Logical Infrastructure Composition and Management

- Main areas of technical development:
  - Physical infrastructure partitioning (information modelling, synchronisation, abstraction,…).
  - Composition of logical optical and IT infrastructures (orchestration,…).
  - Uniform network and IT resources description
  - Flexible and high resolution infrastructure segmentation tools
  - AAA infrastructure for heterogeneous resource provisioning
  - Dynamic logical infrastructure re-planning tools
  - SLA application awareness
- Impact:
  - Make available independent logical infrastructures to network operators and service providers
  - Combine logical infrastructure resources involving multiple infr. providers
  - Support the separation of physical infrastructure ownership and operation

Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

IT and Transport Service Provisioning

- Main areas of technical development:
  - Extended on demand services for joint Network + IT provisioning (based on an enhanced GMPLS+ and PCE+) with SLA awareness and connection services
  - Cross layer network service monitoring and recovery tools.
  - Support of multiple switching technologies under the same NCP.
  - Infrastructure on demand support (resource re-planning and allocation) services to change the underlying controlled infrastructure.
  - Backwards compatibility (ASON/GMPLS and PCE).
  - Dynamic and/or Scheduled provisioning functionalities.
  - Evolved User-to-Network Interface with low level granularity and SLA.
- Impact:
  - End-to-end dynamic reservations of network and IT resources.
  - New future internet architecture with a novel layer structure.

Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

Expected BUSINESS impact

- IaaS approach will strongly impact new business model. Allow network operators offering tailor made services to novel markets.

- Geyser approach will enable telecom operators to access new markets with new business models. Telecom operator will be allowed moving their business towards high value application layers.

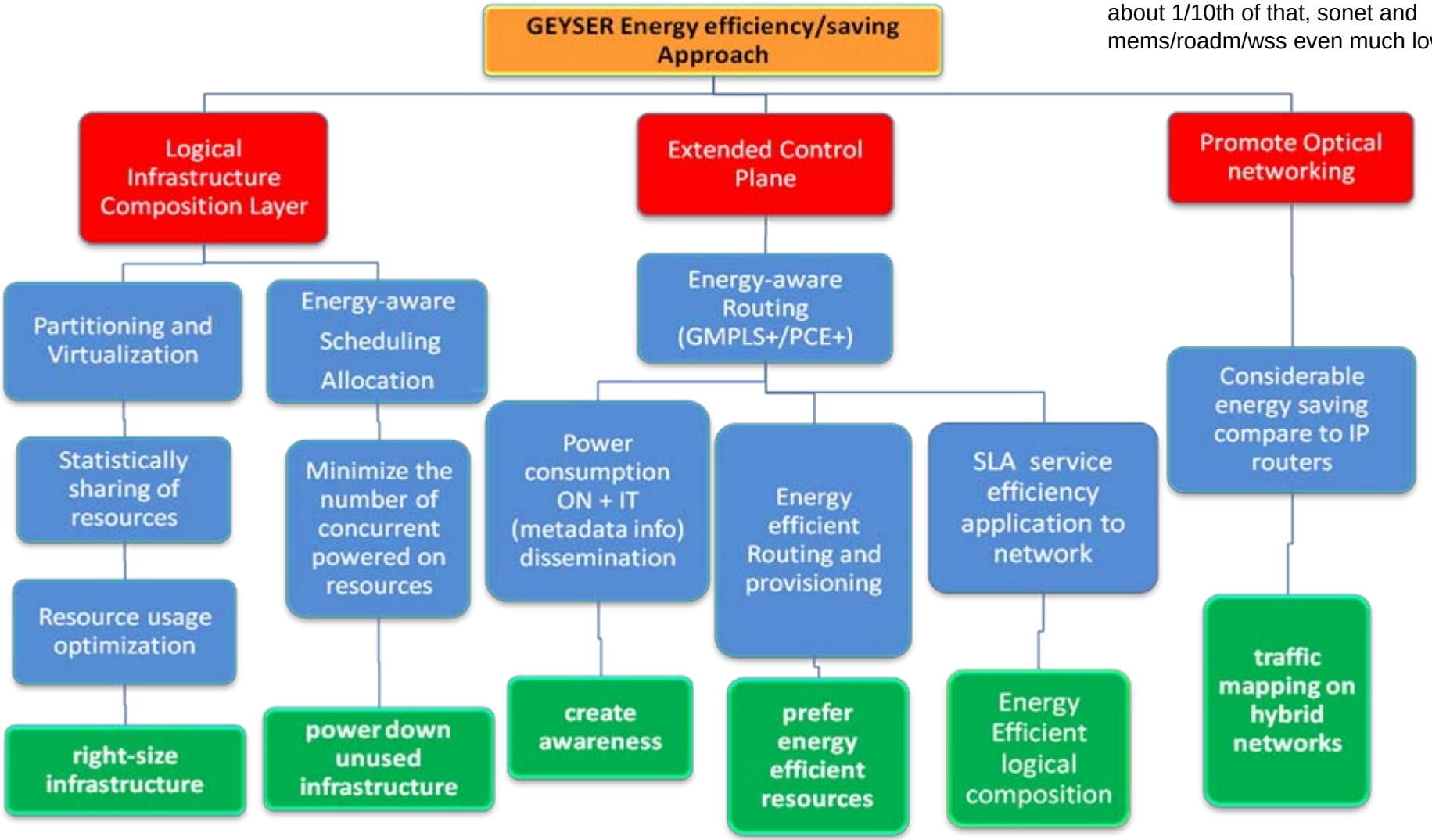
- Geyser concept will allow the development of new actors in ICT environment (existing and emerging Network Operators).

- Application and market expectations will drive the development of new business model based on Geyser concepts and outcomes based on CAPEX and OPEX optimization.

Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

Energy Efficient aspects

router = 250W/10 Gbps, ethernet is about 1/10th of that, sonet and mems/roadm/wss even much lower



Slide from the GEYSERS Project presentation (Courtesy Sergi Figuerola)

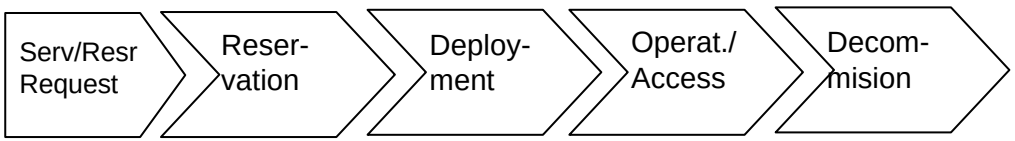
Consistent security services provisioning – Experience and required frameworks

- General requirements – Need for the whole provisioned services life-cycle management and integration with security services
- Services Life-cycle management/support – condition for consistent security services implementation and delivery
- Consistency and correctness of the Security Services design and deployment depends on how well the main service and service provisioning models are defined
  - Re-phrasing “Security strength as a weakest link”:
    Strength and quality of the security services in operation is determined by the weakest stage in the service delivery sequence/framework

Network Resource Provisioning (NRP) Model

4 major stages/phases in NRP operation/workflow

- (Advance) reservation consisting of 3 basic steps
  - Resource Lookup
  - Resource composition (including options)
  - Component resources commitment, including AuthZ/policy decision, and assigning a global reservation ID (GRI)
- Deployment – reservation confirmation and distributing components/domain configuration (including trusted keys distribution)
- Access (to the reserved resource) or consumption
  - Authorisation session management with AuthZ tickets and tokens
- Decommissioning
  - Provisioning session termination
  - Accounting
- *Relocation (under consideration)*



Rationale

- *Supports the whole provisioned resource life-cycle*
- Specifically oriented on combined Grid-Network (heterogeneous) resources provisioning
- Easies Integration of resource provisioning into the upper layer scientific workflow

Security issues in on-demand multi-domain NRP/ISoD

- Main services and Security services life-cycle management
  - Consistent security at each of the composition, deployment, operation stages
- SLA negotiation and support in XACML-NRP
- Inter-domain security context and trust management
  - Using dynamic security associations
- Dynamic security associations creating using
  - DNSSEC Trusted Anchor Repository (TAR)
  - Identity Based Cryptography (IBC)
  - “Leap-of-trust” mechanism – Is it applicable?
- Virtualisation and platform security bootstraping
  - Using TCPA and TPM enabled platforms
- Other issues in multi-domain security services management
  - Identity credentials and attributes
  - Session context and session based credentials
  - Domain policy matching/mapping

What does it mean consistent security services deployment

- Addressing Confidentiality, Integrity, Authenticity properties of the services and data at each life-cycle stage
- Providing consistent AAA (Authentication, Authorisation, Accounting) services integration
  - Consistent security mechanisms for inter-domain security context management used
- Policies and consistent policy management
- Identity and Attribute authorities
- Security and Trust domains establishing and configuration
  - Configuring trusted Certificates, key distribution
- Configuration of the security systems and services
  - At deployment stage and dynamic re-configuration during operation

Useful practical and usecase information can be collected by studying standards and BCP documents by ITU-T, IETF, OASIS, Open Group and industry consortia

Looking for existing frameworks/experiences (1)

Suggested approach – Learn from Telecom industry experience/standards and extend/enrich them with new challenges

- ITU-T standards
  - M: Telecommunication management, including TMN and network maintenance (including M.3050 eTOM framework)
  - X: Data networks, open system communications and security
  - Y: Global information infrastructure, Internet protocol aspects and Next-Generation Networks (NGN)
- TMF standardised frameworks, practices and procedures
  - NGOSS – New Generation (including eTOM)
  - SDF - Service Delivery Framework
  - SLA management
- TMS/IPsphere frameworks and practices
  - IPsphere Framework Specification
  - Interworking Session Services and Resource Management (SSRM)

Looking for existing frameworks/experiences (2)

Other industry consortia experience/standards related to SOA based services development, provisioning and management

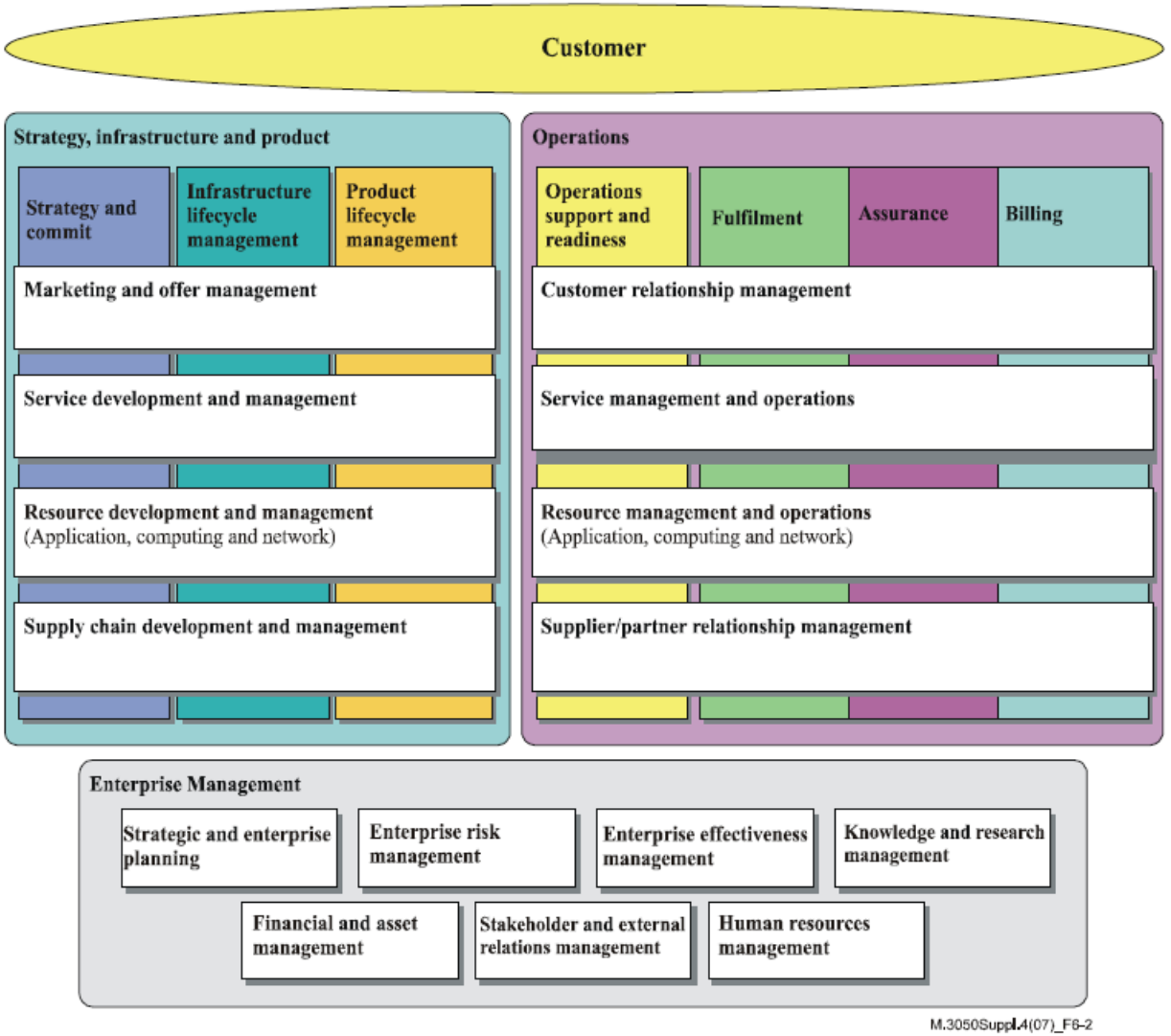
- Open Group Service Integration Maturity Model (OSIMM)
  - Defines 7 maturity level and 7 dimensions
  - Provides framework for evaluation enterprise compliance to SOA model
- TOGAF – The Open Group Architecture Framework)
- OASIS SOA and security related standards
  - Service Components Architecture (SCA) management
    - Including SCA-BPEL, SCA-Policy, SCA-Tel
  - Solution Deployment Descriptor (SDD)
    - Defining a standardized way to express software installation characteristics required for lifecycle management in a multi-platform environment

Looking for existing frameworks/experiences (3)

- IETF
  - Re-evaluate and re-factor COPS (Common Open Policy Service) framework for new Geysers technology platform
- NIST standards defining Security services Design-to-Deployment-to-Operation
- Microsoft Security Development Lifecycle (SDL) Framework
  - “Improving Web Application Security: Threats and Countermeasures” by J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan
  - Primarily focused on the product development process by engineers/programmers

Training – Requirements – Design – Implementation – Verification – Release - Response

TMF/ITU-T Enhanced Telecom Operations Map (eTOM)



Defines Business Process Framework for TeleManagement network operators

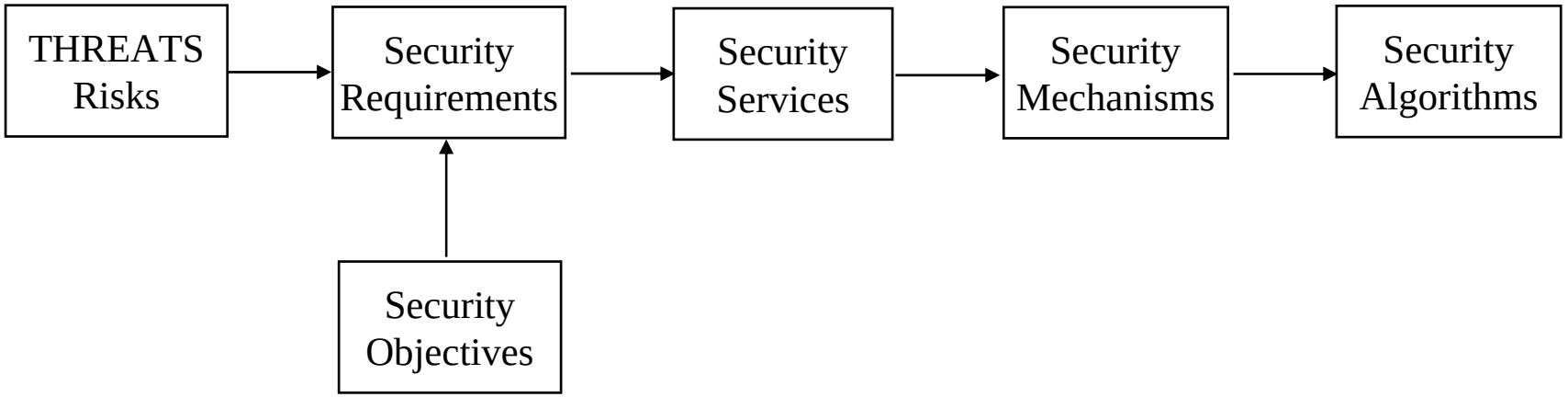
T-REC M.3050.0-M.3050.4

Security is a part of the combined Fault, Configuration, Accounting, Performance and Security (FCAPS) management functional areas

Application to ISoD usecases to be investigated

- Security in services composition and delivery – GN3 JRA3-T3, GEYSERS
- Services operation – GN3 JRA2-T2

TeleManagement Security Framework



Security for Management Plane is defined by the group of standards ITU-T (T-REC) M.3016.0-M.3016.4, M.3410

- Strongly built on the X.800 standards on the Security Architecture for Open Systems Interconnection
- Extends to the Next Generations Network security (Y set of ITU-T recommendations)

ITU-T Y-seria NGN Security Recommendations

- **ITU-T REC Y.2232 (01/2008) NGN convergence service model and scenario using Web Services**

- 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.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

IPSphere Framework

IPsphere is currently a part of the TMF (http://www.tmforum.org/ipsphere)

- The IPsphere Framework delivers a business layer for rapid service delivery, including advanced support for IP services. Using the principles of a service-oriented architecture (SOA), the IPsphere Framework defines mechanisms to automate offers, purchase and provision service components among multiple stakeholders, enabling providers to optimize flexibility and efficiency

IPSphere documents

- IPsphere Framework Technical Specification
- Interworking Session Services and Resource Management (SSRM)
  - Has a good description of the session based security

TMF Solutions Framework NGOSS

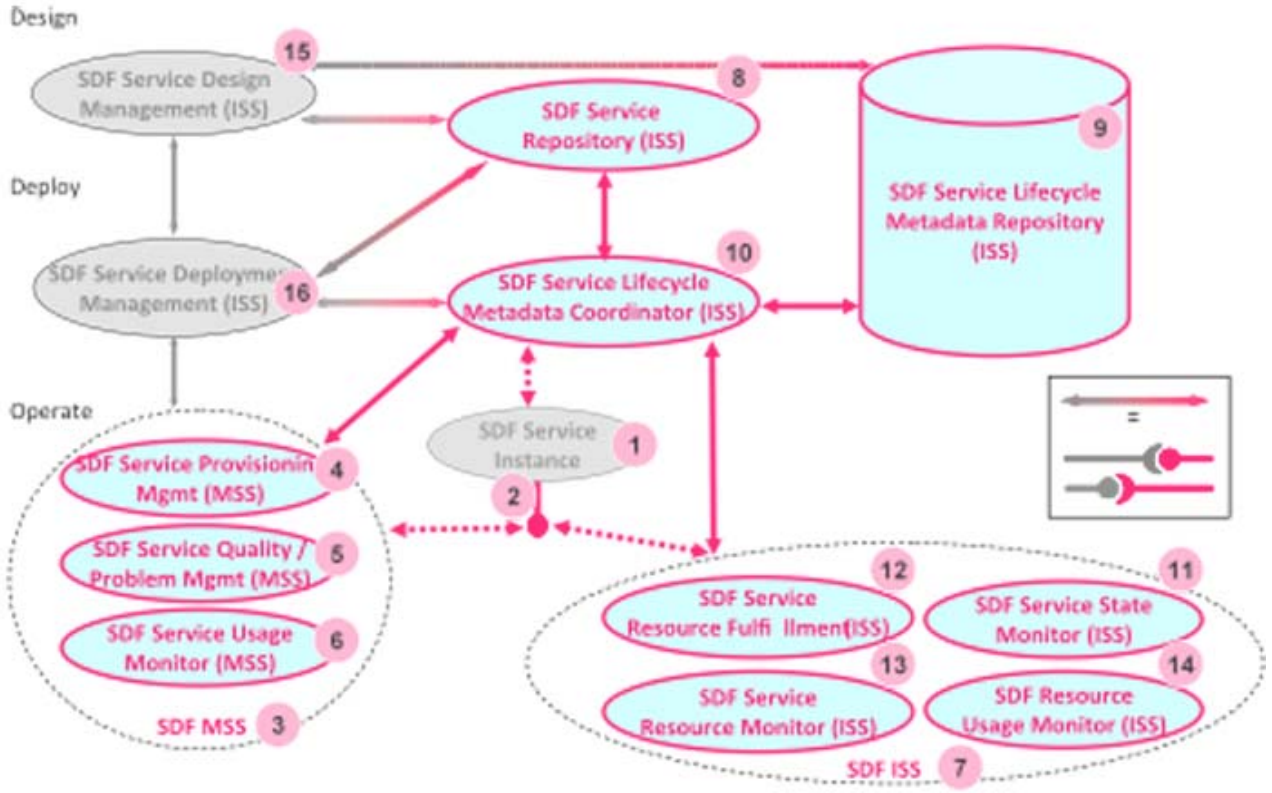
- NGOSS - New Generation Operations Systems and Software principles (http://www.tmforum.org/BestPracticesStandards/ServiceDeliveryFramework/4664/Home.html)
  - Separation of Business Process from Component Implementation
  - Loosely Coupled Distributed System
  - Shared Information Model
  - Common Communications Infrastructure
  - Contract defined interfaces
- NGOSS lifecycle divides systems development into 4 stages: requirements, system design, implementation and operation
- eTOM is a component of NGOSS

TMF Service Delivery Framework (SDF)

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

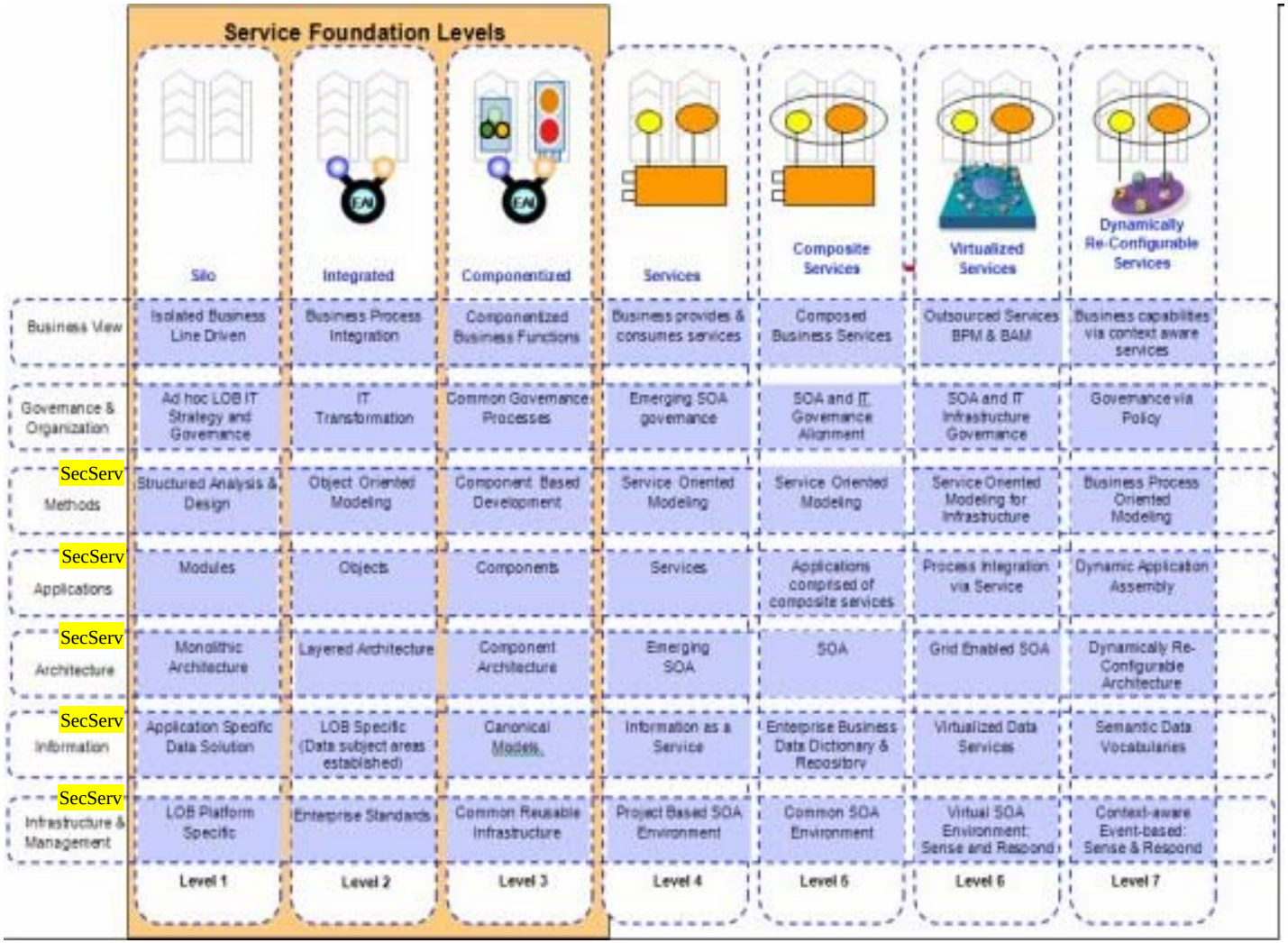
- End-to-end service management in a multi-service providers environment
- End-to-end service management in a composite, hosted and/or syndicated service environment
- Management functions to support a highly distributed service environment, for example unified or federated security, user profile management, 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



1 – SDF Service Instance
2 - Service Management Interface
3 - Management Support Service (SDF MSS)
7 - Infrastructure Support Service (ISS)
DESIGN stage
8 - Service Repository
9 - Service Lifecycle Metadata Repository
15 - Service Design Management
DEPLOYMENT stage
9 - Service Lifecycle Metadata Repository
10 - Service Lifecycle Metadata Coordinator
16 - Service Deployment Management
OPERATION stage
4 - Service Provisioning Management
5 - Service Quality/Problem Management
6 - Service Usage Monitor
11 - Service State Monitor
12 - Service Resource Fulfillment
13 - Service Resource Monitor
14 - Resource Usage Monitor

The Open Group Service Integration Maturity Model (OSIMM)



Provides framework for evaluation and development strategy for building SOA compliant services and business model/processes migration to true SOA

- Defines 7 maturity level and 7 dimensions

To ensure consistency, security issue (security domain) to be addressed at dimensions:

- Business
- Methods/models
- Services
- (Information)

Source: IBM - http://www.ibm.com/developerworks/webservices/library/ws-OSIMM/index.html

OSIMM Maturity Levels and Dimensions

Maturity levels 1…7

- Silo
- Integrated
- Componentised
- Services
- **Composable services**
- Virtualised services
- **Dynamically re-configurable services**

Dimensions 1…7

- Business view
- Governance and Operations
- Methods
- Applications
- Architecture
- Information
- Infrastructure and Management

- Domains are defined as a specific problem area and are projected into Maturity – Dimensions grid
  - Security services
  - Management services
- Services Lifecycle management should be a part the domain definition
  - Allows for combining higher level services definition and lower level interfaces deployment

TOGAF – The Open Group Architecture Framework (1)

TOGAF embrace ISO/IEC 42010: 2007 definition of ‘‘architecture’’:

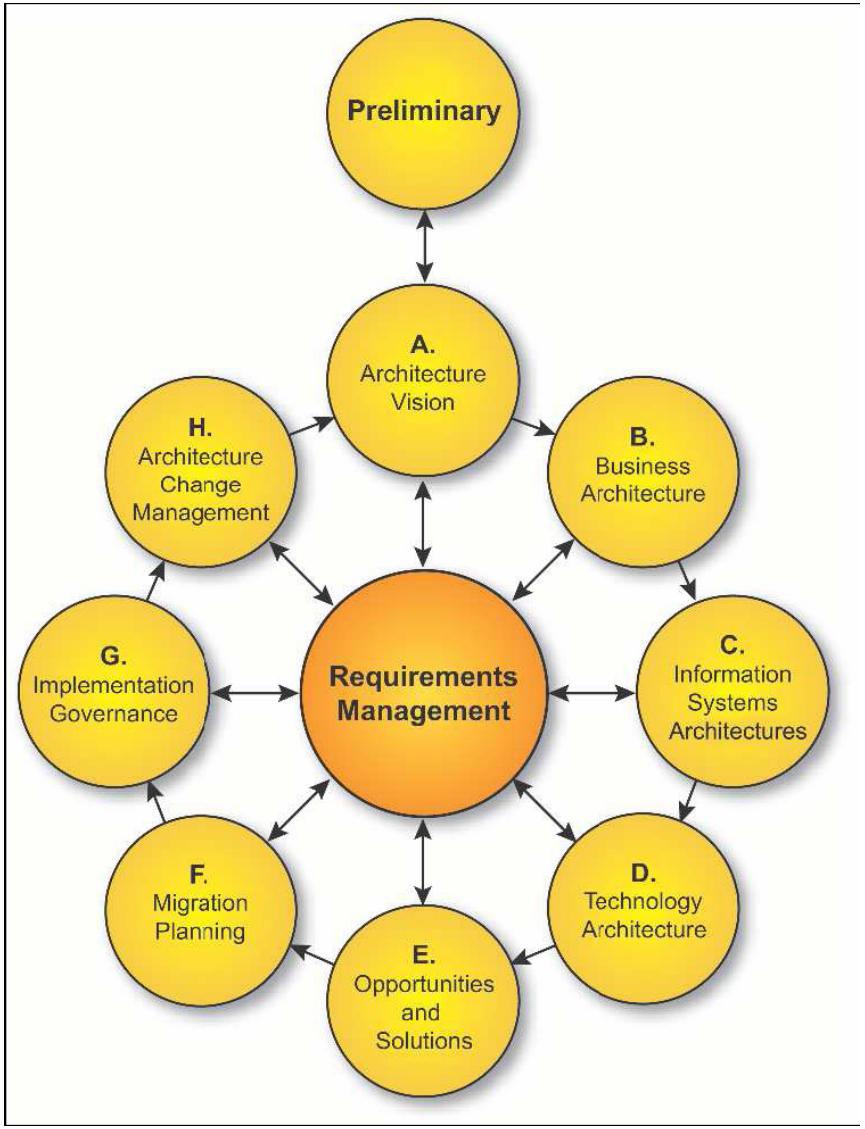
‘‘The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.’’

- Business Architecture
- Data Architecture
- Application Architecture
- Technology Architecture

Developer-led SOA asks: “What is the best way to design, build, and operate services?”

Business-led SOA asks: “What services are needed and how should they be governed and fulfilled?”

TOGAF – The Open Group Architecture Framework (2)



The Preliminary Phase

Phase A: Architecture Vision

Phase B: Business Architecture

Phase C: Information Systems Architectures – Data and Applications

Phase D: Technology Architecture

Phase E: Opportunities & Solutions

Phase F: Migration Planning

Phase G: Implementation Governance

Phase H: Architecture Change Management

Requirements Management

NIST SP800-14 (1996), SP800-27 (2006)

SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems – Lifecycle planning phases

- Initiation Phase
- Development/Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase

Proposed Security Services Lifecycle Management Model

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.

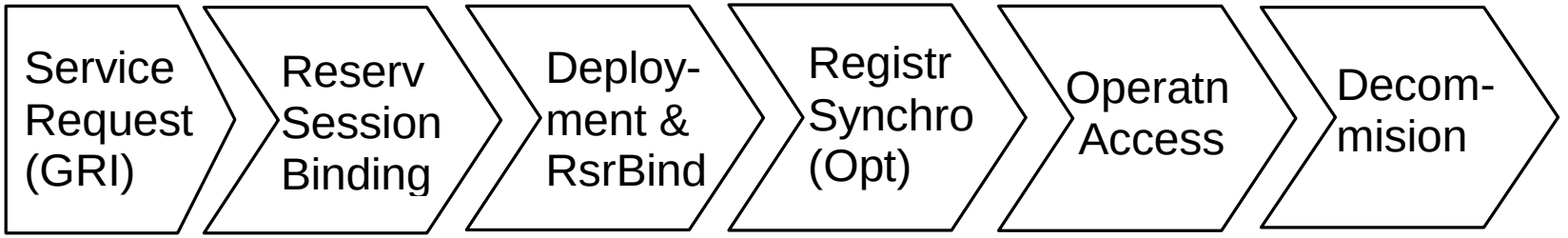
Reservation session binding that provides support for complex reservation process including required access control and policy enforcement.

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) that 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.



Suggested future research and developments

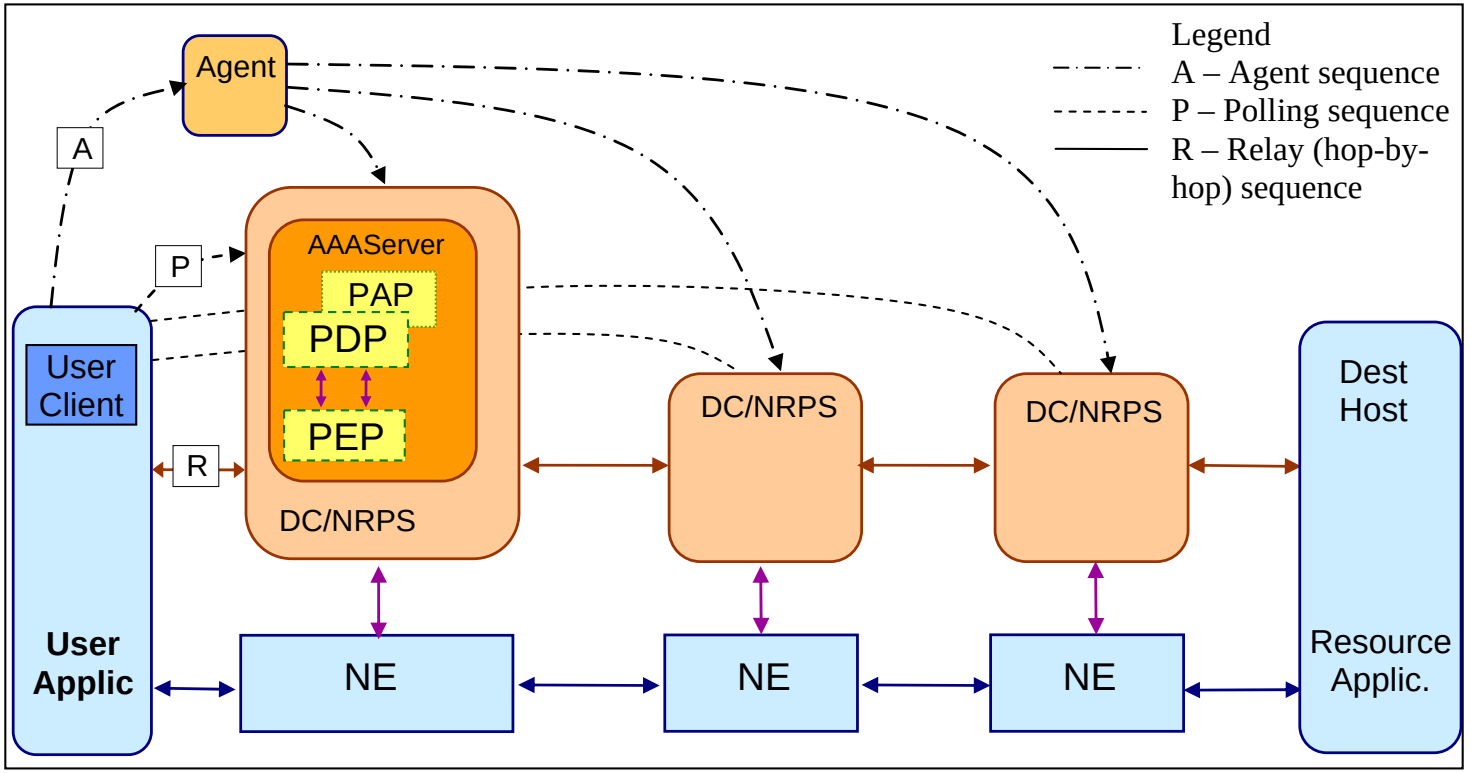
- Review Clouds technologies security as move computing to infrastructure service
- Review Telecom industry standards by ITU-T, TMF, IPsphere
  - Position ISoD framework against ITU-T and TMF frameworks/models
- Formalising ISoD/NRP and dynamic/on-demand services delivery lifecycle and supporting workflow targeting basic usecases
  - Composable services and GEMBus in GN3 JRA3-T3
  - Virtualised infrastructure provisioning in GEYSERS project
- Defining network topology aware XACML-NRP policy model and contributing a usecase to OGF NML-WG
- Developing trust model for NRP and investigate technologies for cross-domain trust management
  - Identity Based Cryptography (IBC)
  - DNSSEC Trusted Anchors Repository (TAR)

Discussion and Questions

Additional Materials

- Authorisation infrastructure for NRP
- Authorisation Tokens for security session management

Multidomain Network Resource Provisioning (NRP) – Provisioning sequences



Provisioning sequences

- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement

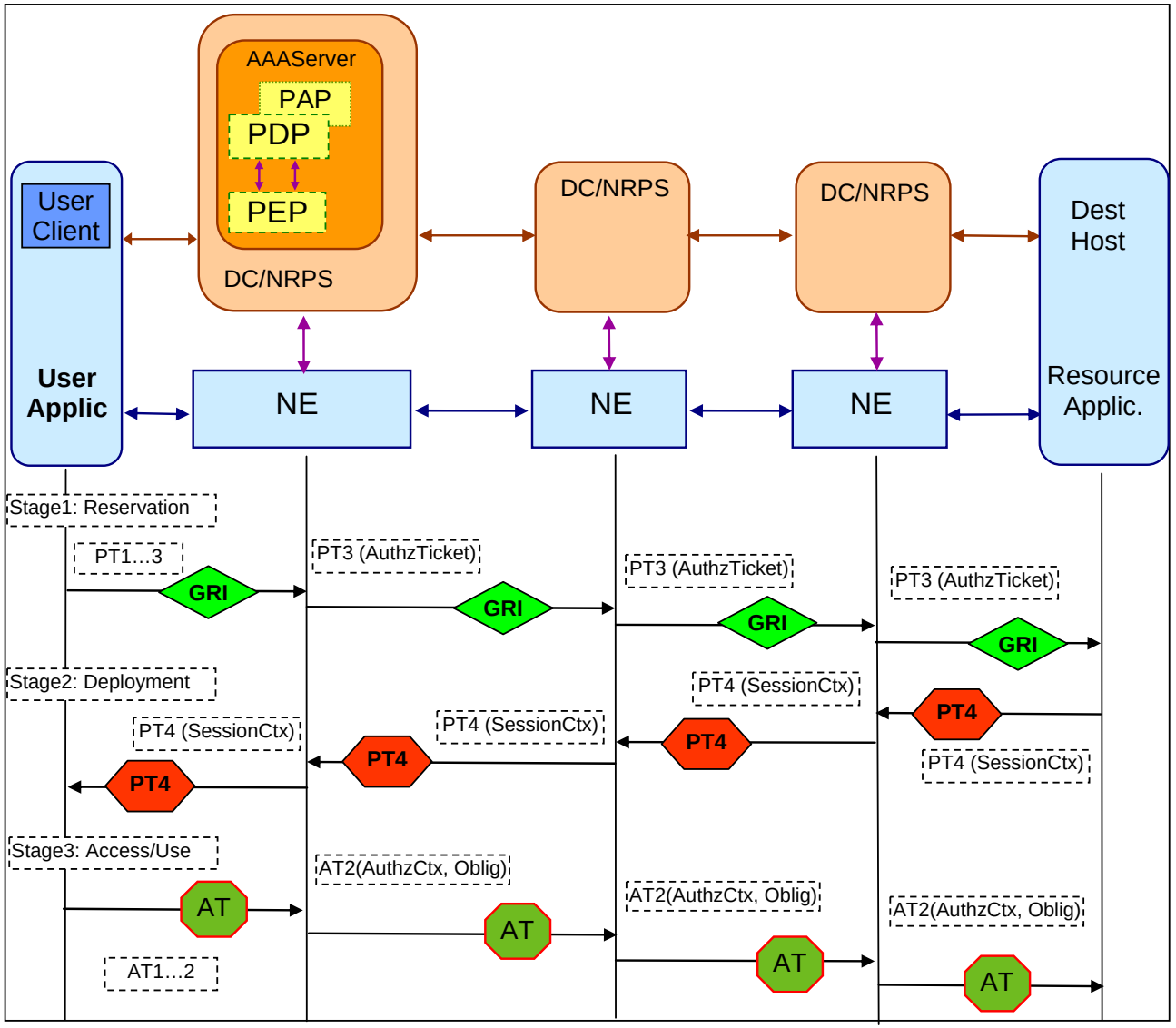
GRI – Global Reservation ID

AuthZ tickets for multidomain context mngnt

PT- Pilot tokens for signaling and access control

- AAA – AuthN, AuthZ, Accounting Server
- PDP – Policy Decision Point
- PEP – Policy Enforcement Point
- NRPS – Network Resource Provisioning System
- DC – Domain Controller

Multidomain Network Resource Provisioning (NRP) – Stage 1 – Path building and Advance Reservation



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT1…2 – Access Token

PT1…3 Pilot token type 1…3 used at the Stage 1 Reservation

PP4 Pilot Token type 4 used at the Stage 2 Deployment

DC – Domain Controller

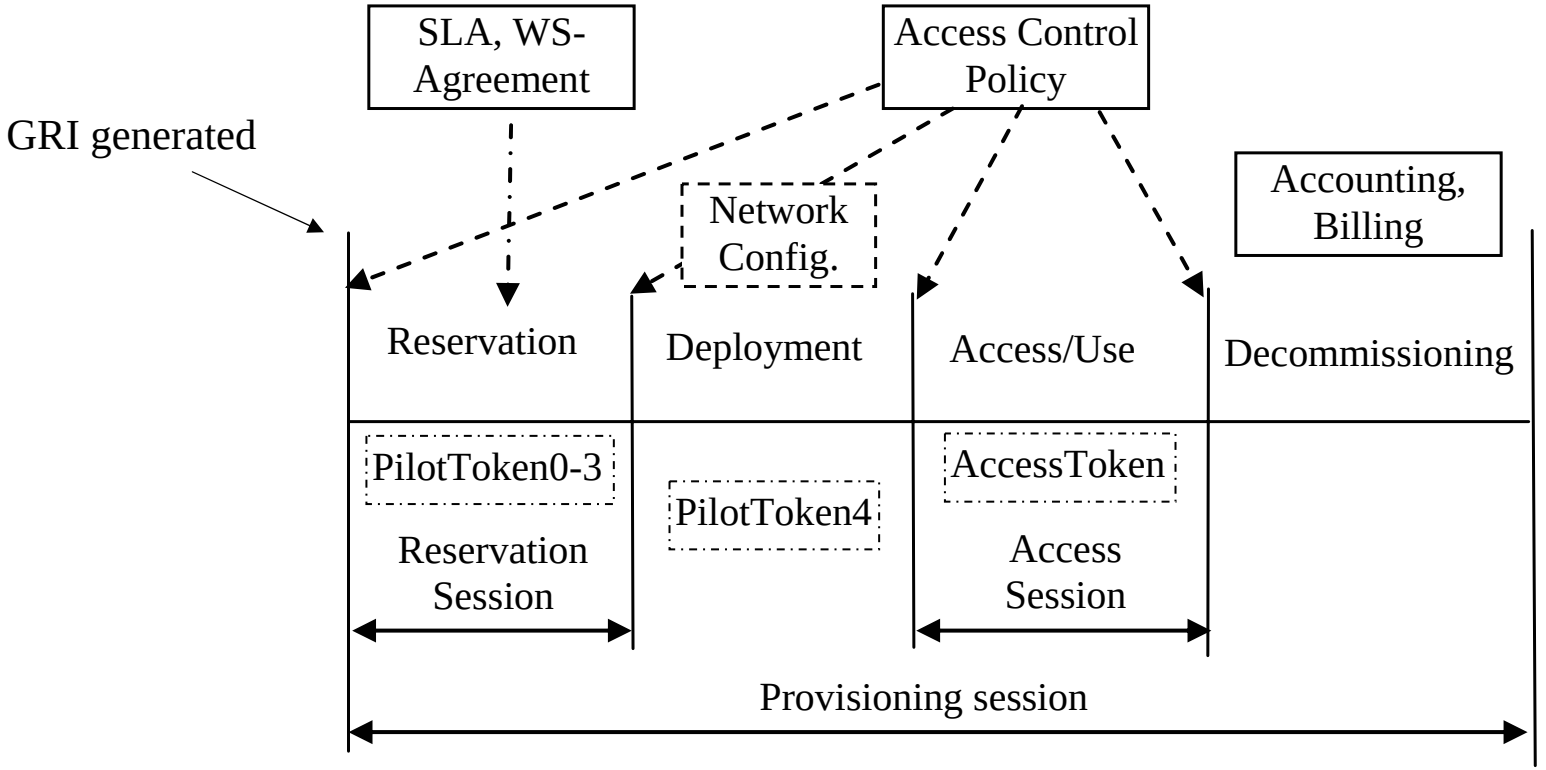
NRPS – Network Resource Provisioning System

NE - Network Element AAA – AuthN, AuthZ, Accounting Server

PEP – Policy Enforcement Point

PDP – Policy Decision Point

NRP Stages and Authorisation Session Types



Requires consistent security and session context management

Global Reservation ID (GRI) is created at the beginning of the provisioning session (Reservation stage) and binds all sessions

AAA/AuthZ mechanisms and functional components to support multidomain NRP

The proposed AAA/security mechanisms and functional components to extend generic AAA AuthZ framework (PEP, PDP, PAP and operational sequences)

Token Validation Service (TVS) to enable token based policy enforcement

- Can be applied at all Networking layers (Service, Control and Data planes)
- *Pilot Token signalling mechanism implemented in the GAAA-TK library*

AuthZ ticket format for extended AuthZ session management

- To allow extended AuthZ decision/session context communication between domains

XACML-NRP attributes and policy profile for NRP

- Rich functionality of the XACML policy format for complex network and Grid resources
- *Can add dynamic path/topology information and Policy obligations to policy definition*

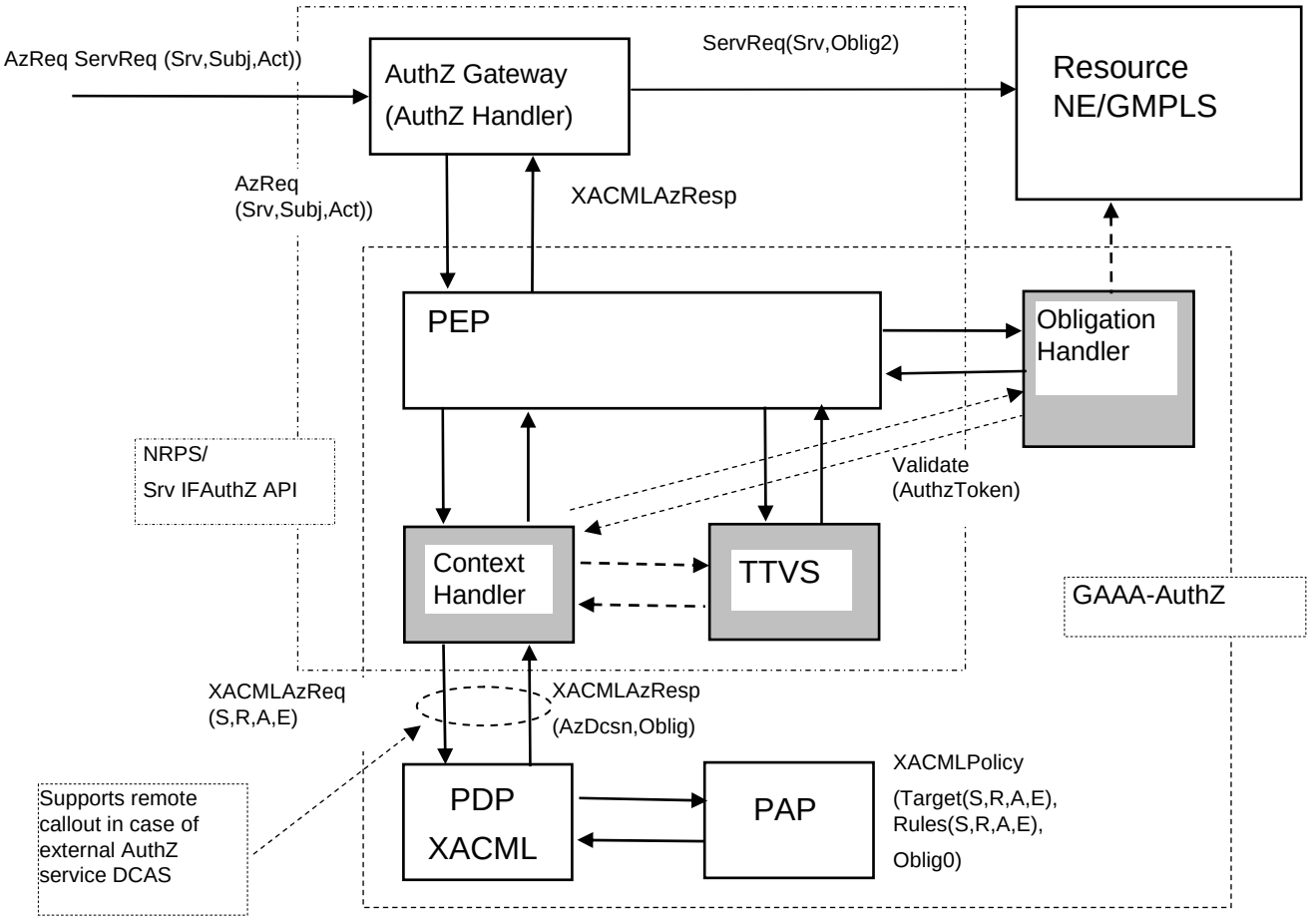
Policy Obligation Handling Reference Model (OHRM)

- Used for account mapping, quota enforcement, accounting, etc.

The proposed architecture allows smooth integration with other AuthZ frameworks as currently used and being developed by NREN and Grid community

- Can provide basic AAA/AuthZ functionality for each network layer DP, CP, SP

GAAA Toolkit pluggable AAA/AuthZ components



The proposed model intends to comply with both the generic AAA-AuthZ framework and XACML AuthZ model

- ContextHandler functionality can be extended to support all communications between PEP-PDP and with other modules
- Obligation Handler supports OHRM
- TTVS supports session based credentials – Access and Pilot tokens and tickets

TTVS – Ticket and token validation and handling service

Access Token and Pilot Token Types

AType 0 – Simple access token (refers to the reserved resources context)

AType 1 – Access token containing Obligations

PType 1 – Container for communicating the GRI during the reservation stage

- Contains the mandatory SessionId=GRI attribute and an optional Condition element

PType 2 – Origin/requestor authenticating token

- TokenValue element contains a value that can be used as the authentication value for the token origin
- TokenValue may be calculated of the (GRI, IssuerId, TokenId) by applying e.g. HMAC function with the requestor's symmetric or private key.

PType 3 – Extends Type 2 with the Domains element that allows collecting domains security context information when passing multiple domains during the reservation process

- Domains' information may include the previous token and the domain's trust anchor or public key
- Can include also AuthZ ticket for extended AuthZ context communication

PType 4 – Used at the deployment stage and can communicate between domains security context information about all participating in the provisioned lightpath or network infrastructure resources

- Can be used for programming/setting up a TVS infrastructure for consistent access control tokens processing at the resource access stage