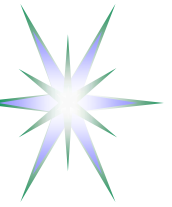


Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning

Yuri Demchenko
SNE Group, University of Amsterdam

ISOD BOF, OGF28, 15 March 2010



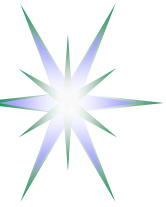
Outline

- Background research and development
 - ◆ GAAA-NRP for Network Resource Provisioning
 - ◆ GN3-JRA3-T3 Composable services
 - ◆ AAA/Security infrastructure for on-demand Infrastructure resources provisioning in the GEYSERS project
- Security issues in on-demand services provisioning
- Standardisation in Service/Resource Operations and Delivery
 - ◆ ITU-T, TMF, IPsphere, OpenGroup, OASIS
- Proposed Security Services Lifecycle Management Model
- Suggested contribution to the ISOD WG



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



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)*



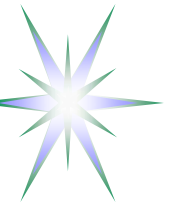
Rationale

- *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

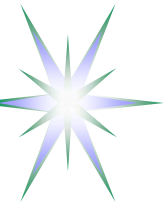
- Main services and Security services life-cycle management
 - ◆ Consistent security at each of the composition, deployment, operation stages
- SLA negotiation and support in XACML-NRP
- Inter-domain security context and trust management
 - ◆ Using dynamic security associations
- Dynamic security associations creating using
 - ◆ DNSSEC Trusted Anchor Repository (TAR)
 - ◆ Identity Based Cryptography (IBC)
 - ◆ “Leap-of-trust” mechanism – Is it applicable?
- Virtualisation and platform security bootstrapping
 - ◆ 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



Consistent security services - What does it mean?

- 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

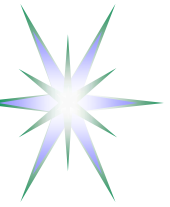
Useful practical and usecase information can be collected by studying standards and BCP documents by ITU-T, IETF, OASIS, Open Group and industry consortia



Existing frameworks/standards (1)

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

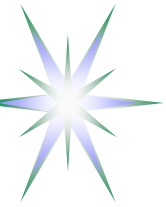
- ITU-T standards
 - ◆ M: Telecommunication management, including TMN and network maintenance (including M.3050 eTOM framework)
 - ◆ X: Data networks, open system communications and security
 - ◆ Y: Global information infrastructure, Internet protocol aspects and Next-Generation Networks (NGN)
- TMF 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)



Existing frameworks/standards (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



Existing frameworks/standards (3)

- IETF/IRTF
 - ◆ Re-evaluate and re-factor COPS (Common Open Policy Service) framework for new Geysers technology platform
 - ◆ Network Virtualisation Research Group (NVRG)
 - Primarily focused on Network layer network virtualisation and OS based virtualisation of network services
 - Doesn't consider the overall network infrastructure service virtualisation
- NIST standards defining Security services Design-to-Deployment-to-Operation
 - ◆ 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



Existing frameworks/standards (4)

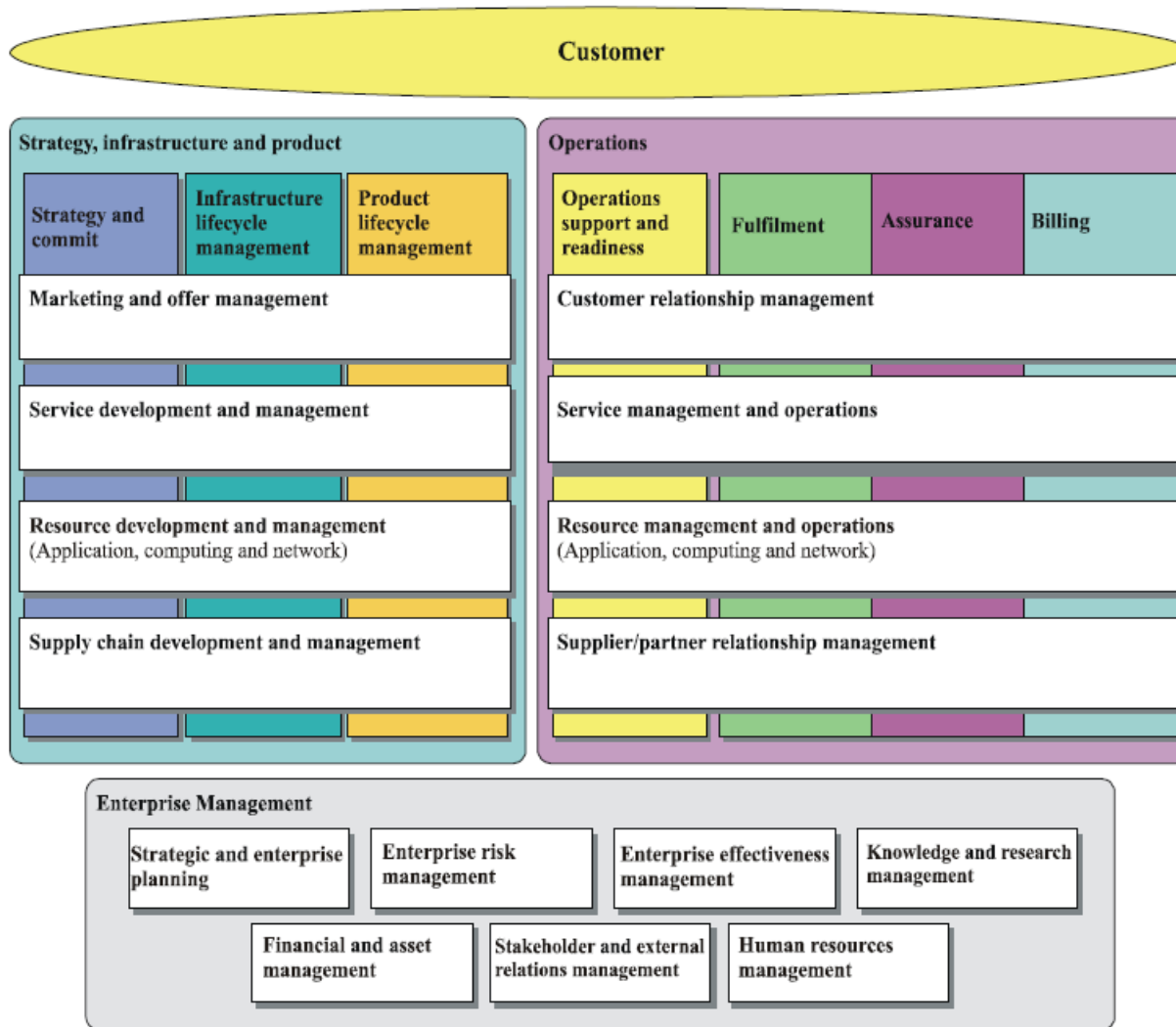
- Microsoft Security Development Lifecycle (SDL) Framework
 - ◆ “Improving Web Application Security: Threats and Countermeasures” by J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan
 - ◆ Primarily focused on the product development process by engineers/programmers

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

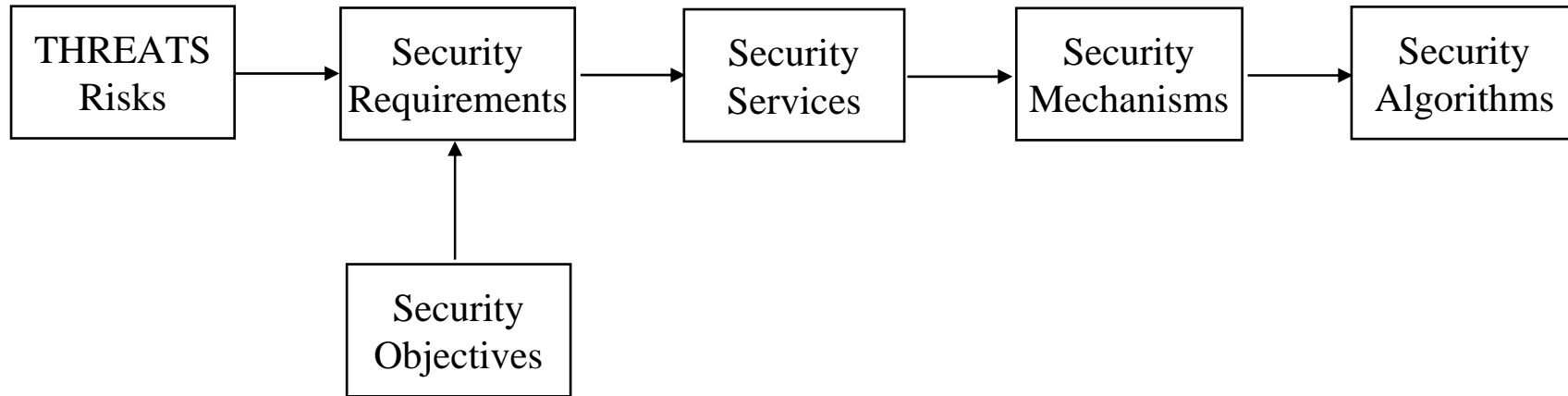
Application to ISoD usecases to be investigated

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

M.3050Suppl4(07)_F6-2



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



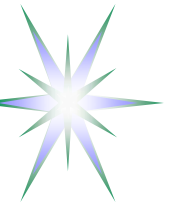
IPSphere Framework

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

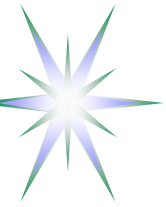
IPSphere documents

- 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

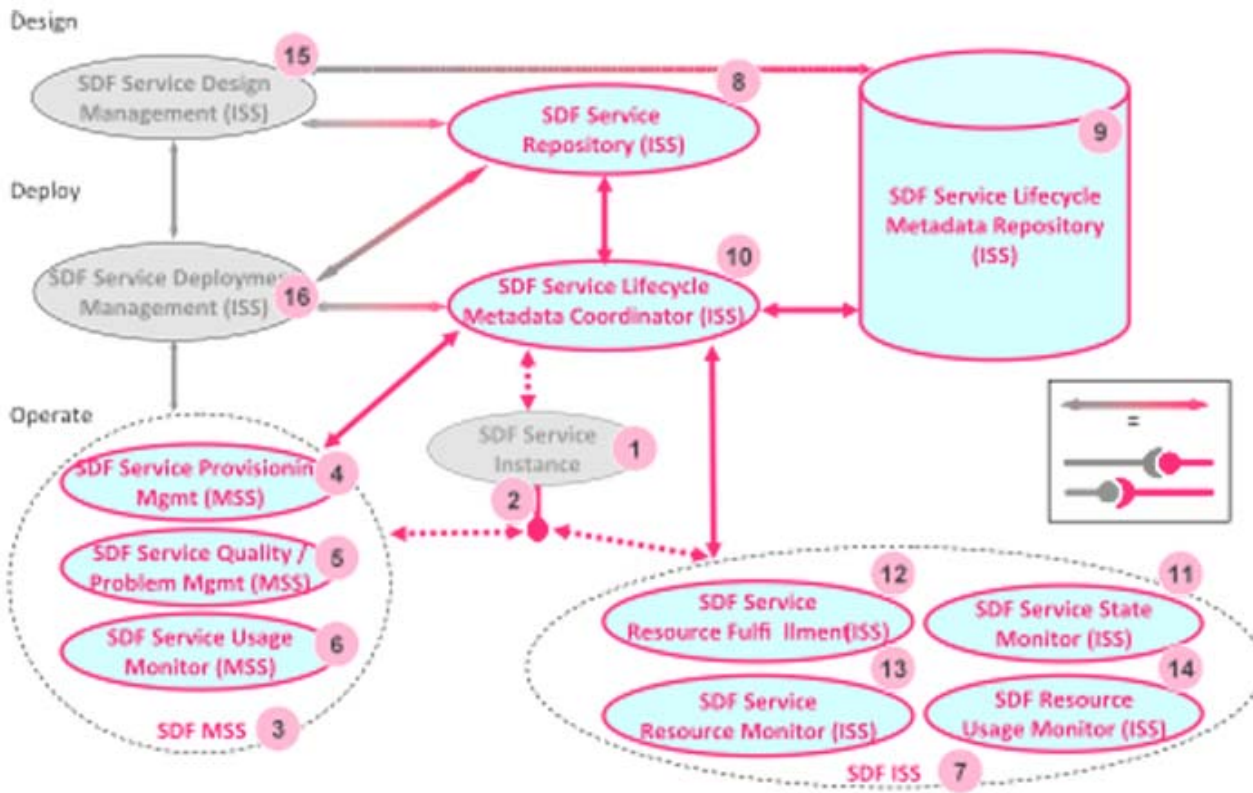
- End-to-end service management in a multi-service providers environment
- End-to-end service management in a composite, hosted and/or syndicated service environment
- Management functions to support a highly distributed service environment, for example unified or federated security, user profile management, charging etc.
- Any other scenario that pertains to a given phase of the service lifecycle challenges, such as on-boarding, provisioning, or service creation

Service Delivery Lifecycle

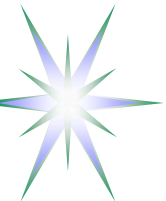




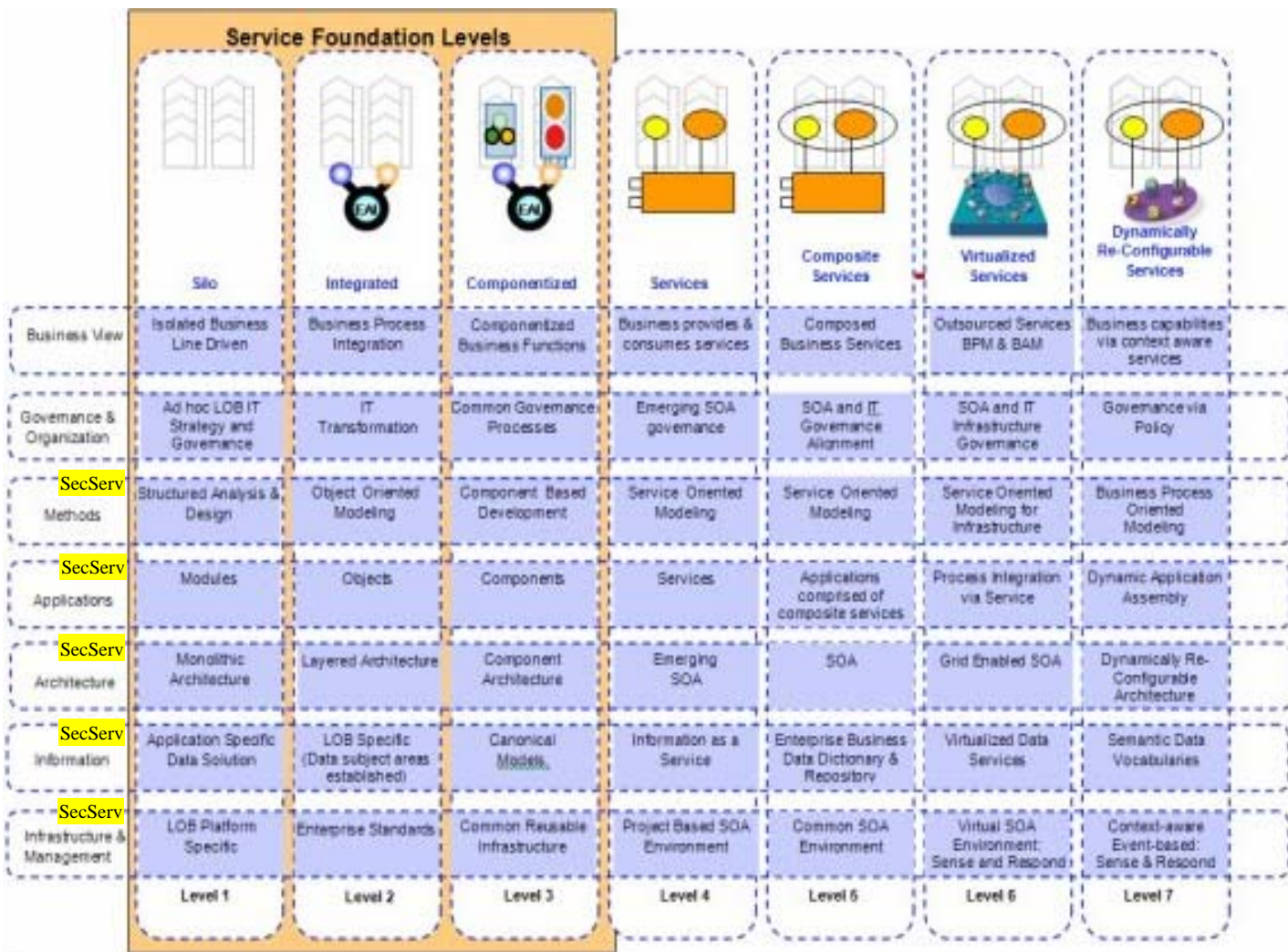
SDF Reference Architecture



- 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)



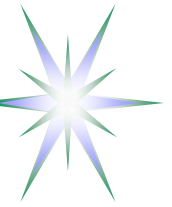
Provides framework for evaluation and development strategy for building SOA compliant services and business model/processes migration to true SOA

- 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

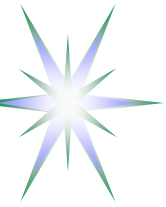
Maturity levels 1...7

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

- 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

Dimensions 1...7

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



Proposed Security Services Lifecycle Management 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.

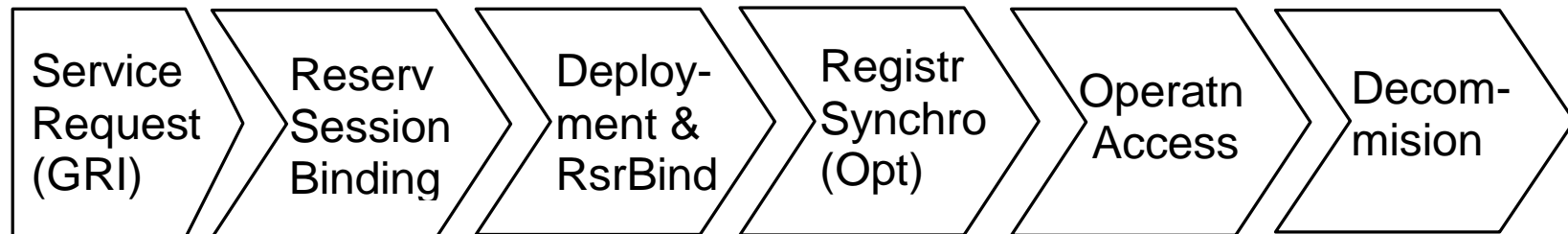
Reservation session binding that provides support for complex reservation process including required access control and policy enforcement.

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.

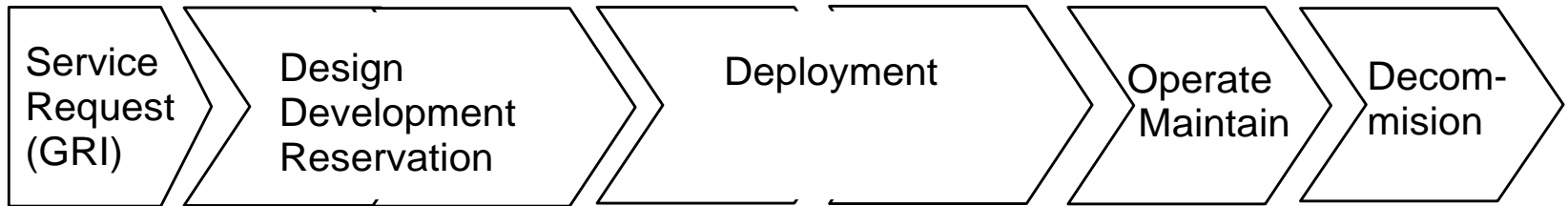
Decommissioning stage ensures that all sessions are terminated, data are cleaned up and session security context is recycled.



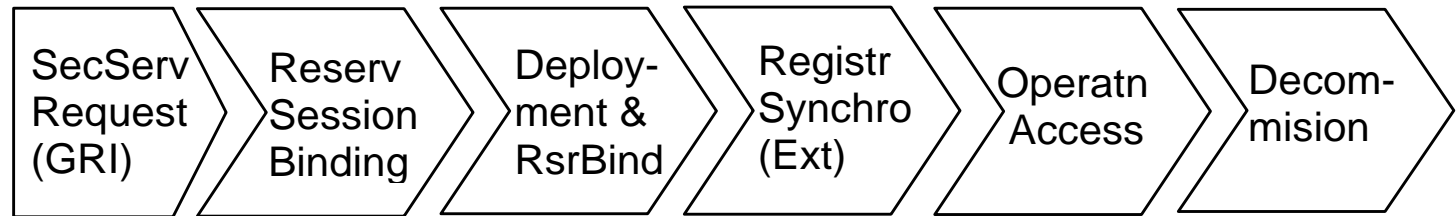


Relation between SSLM and general SLM

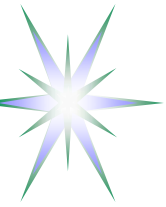
(a) Services Lifecycle Stages



(b) Security Services Lifecycle Stages

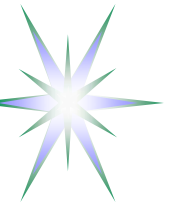


- Service Request stage may include SLA negotiation
 - ◆ Security service instantiation may use SLA security context



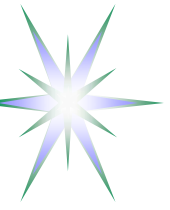
Relation between SSLM/SLM stages and supporting general and security mechanisms

SLM stages	Request	Design/Reservation Development	Deployment	Operation	Decommissioning
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



Suggested contribution to the ISOD WG

- Review Clouds technologies security as a trend to move computing resources 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



Discussion and Questions