Security
in
On-demand Network Resource Provisioning

Yuri Demchenko
SNE Group, University of Amsterdam

On-demand Infrastructure Services Provisioning (ISoD) Workshop
8 December 2009, Amsterdam

Outline

- Background - Projects and developments
  - Network Resource Provisioning model/workflow
  - Generic AAA/AuthZ Infrastructure for multi-domain Network Resource Provisioning (GAAA-NRP) – Phosphorus project
- Security issues in on-demand NRP
- Standardisation in Service/Resource Operations and Delivery
  - IPsphere, TMF, ITU-T
- 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

Experiences and required frameworks for consistent security services provisioning

- 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

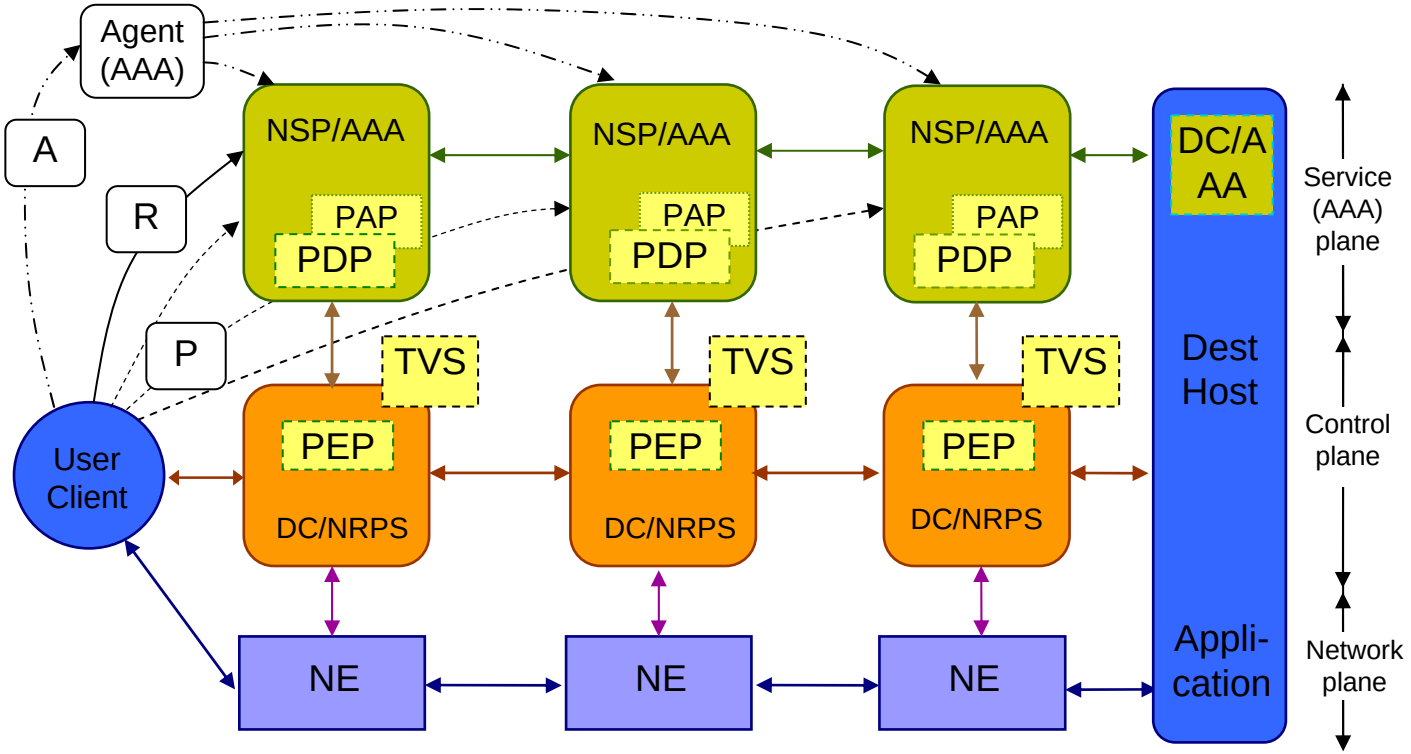
4 major stages/phases in NRP operation/workflow

- (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

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

T - Token

NRPS – Network Resource Provisioning System

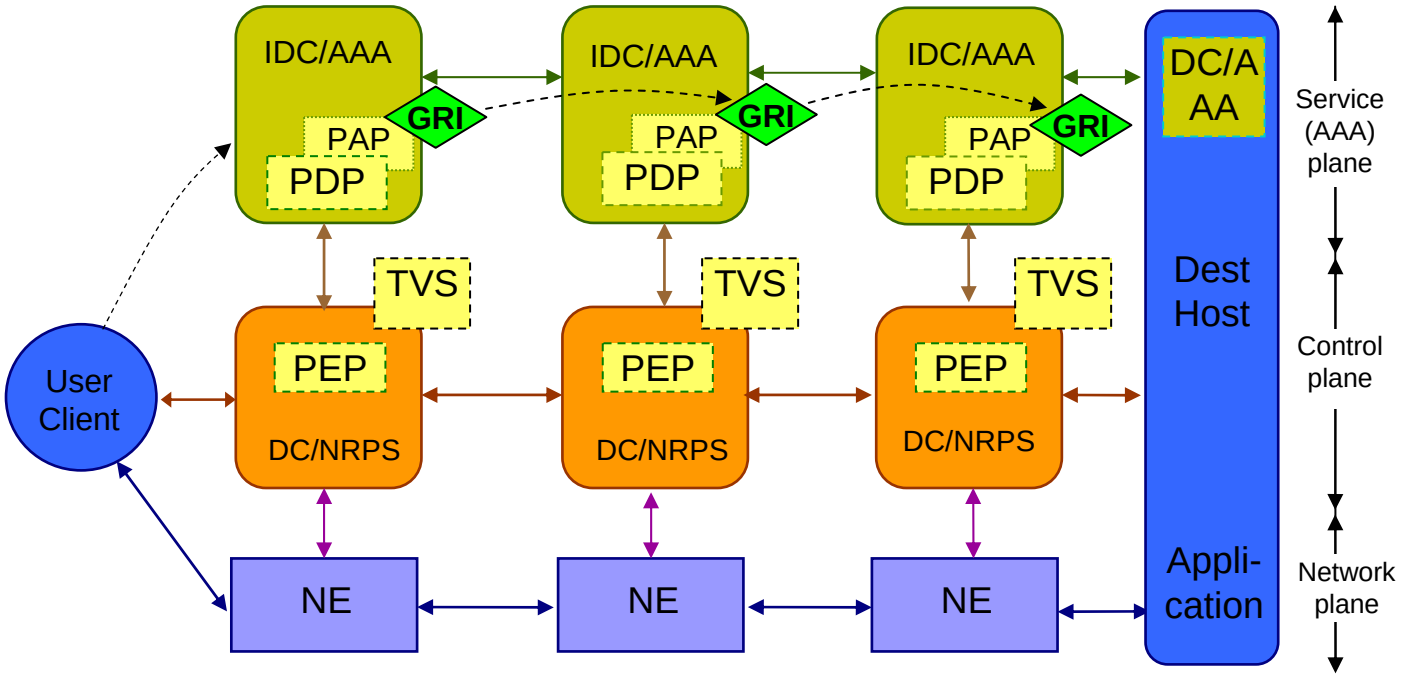
NSP – Network Service Plain

DC – Domain Controller

IDC – Interdomain Controller

- AAA – AuthN, AuthZ, Accounting Server
- PDP – Policy Decision Point
- PEP – Policy Enforcement Point
- TVS – Token Validation Service
- KGS – Key Generation Service

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

AT – Access Token

Pilot Token type 3 used at the Stage 1 Reservation for signalling and interdomain context communication

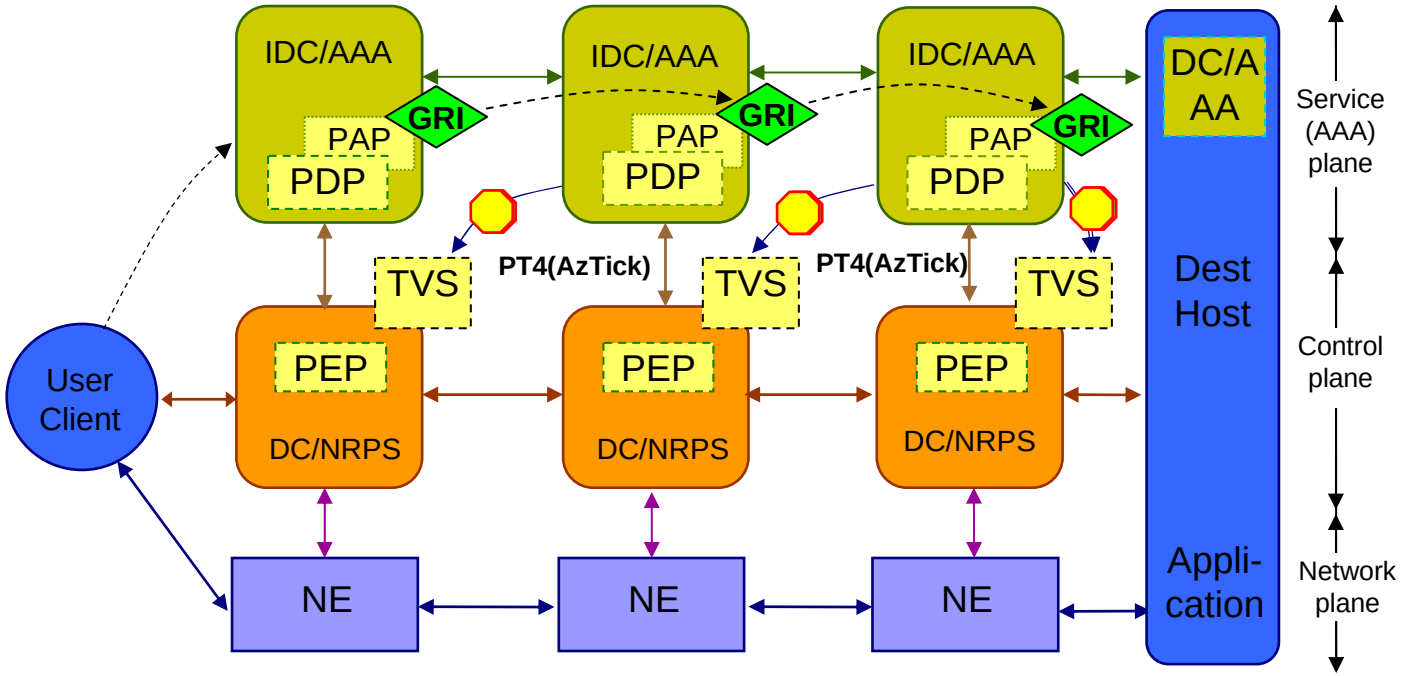
* As container for GRI and AzTicket

Pilot Token type 4 used at the Stage 2 for setup information communication

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service

Multidomain Network Resource Provisioning (NRP) – Stage 2 – Deployment (setup and key distribution)



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT – Access Token

Pilot Token type 3 used at the Stage 1 Reservation for signalling and interdomain context communication

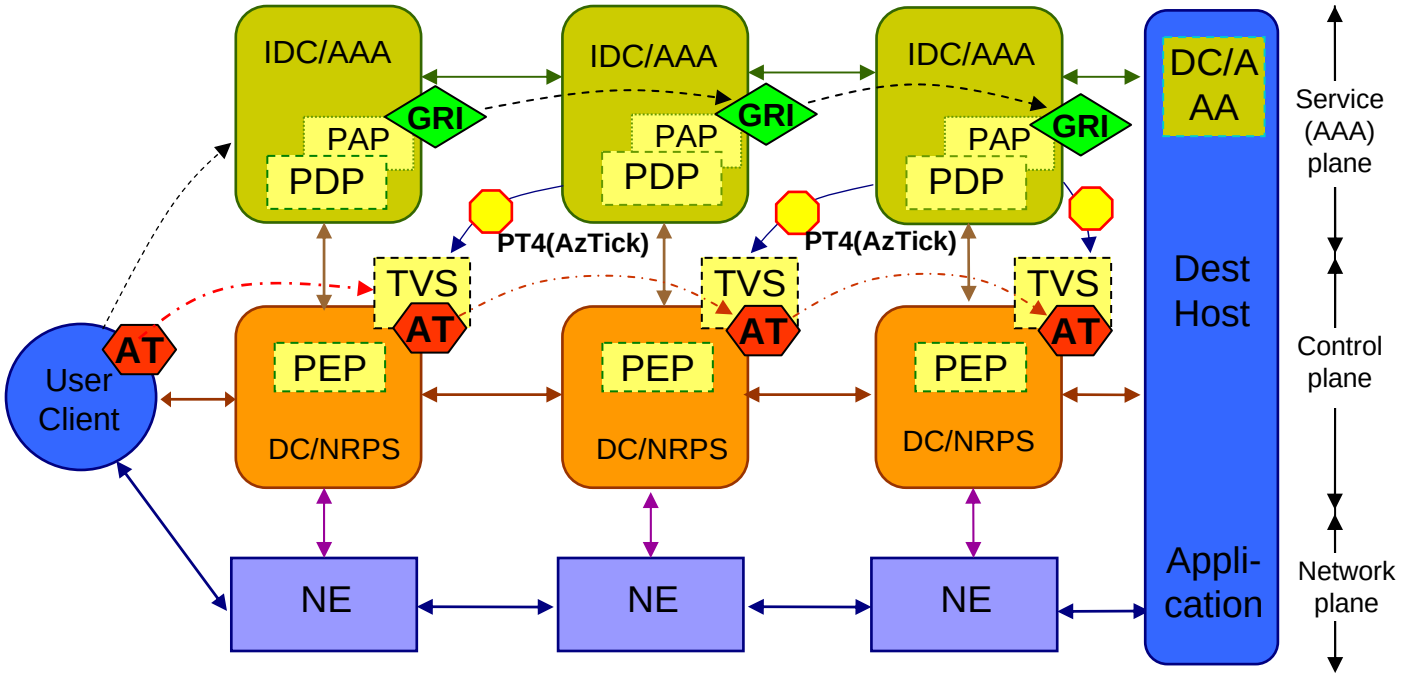
* As container for GRI and AzTicket

Pilot Token type 4 used at the Stage 2 for setup information communication

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service

Multidomain Network Resource Provisioning (NRP) – Stage 3 – Access Control (using access tokens)



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT – Access Token

Pilot Token type 3 used at the Stage 1 Reservation for signalling and interdomain context communication

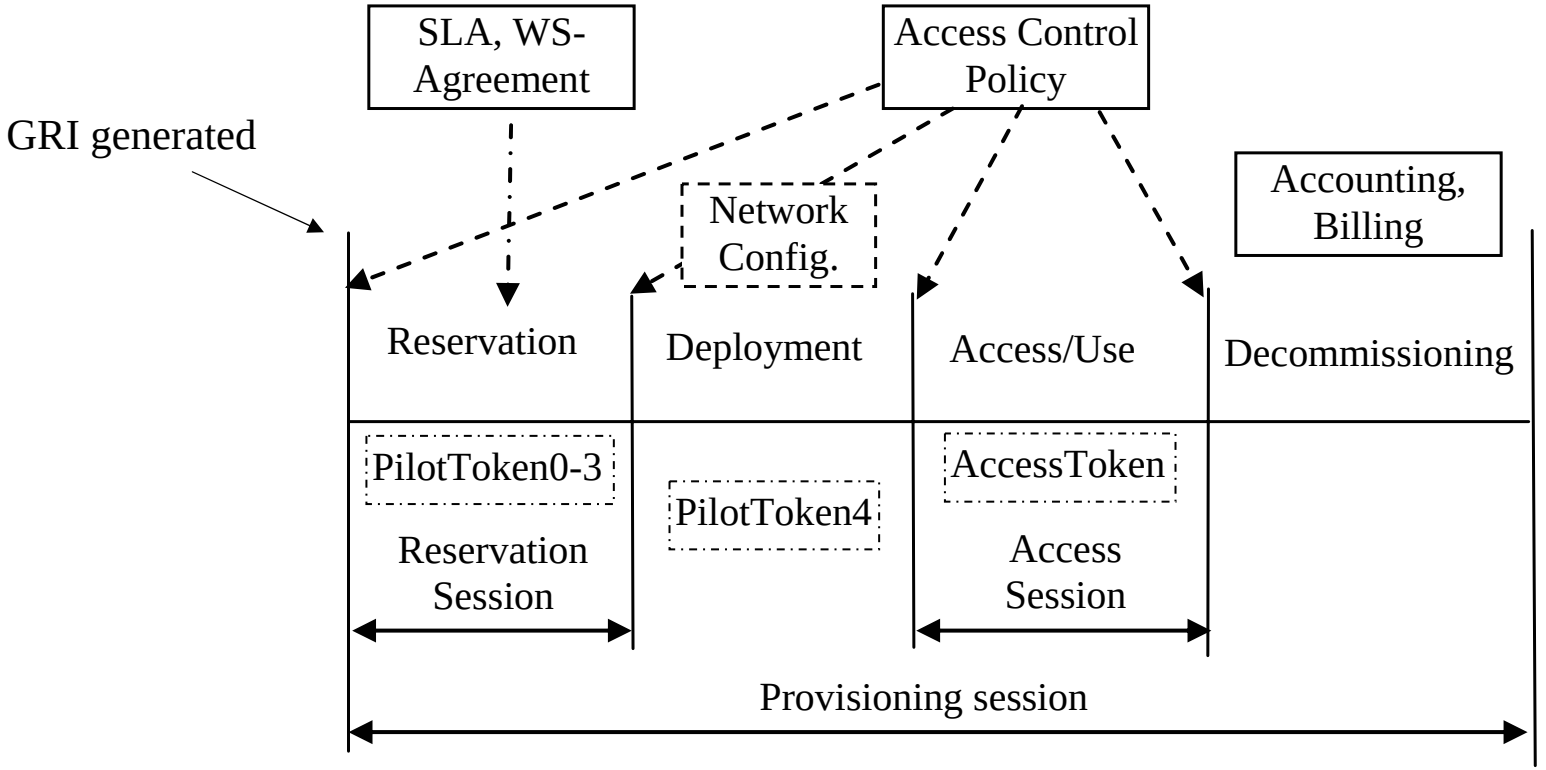
* As container for GRI and AzTicket

Pilot Token type 4 used at the Stage 2 for setup information communication

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service

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

XACML-NRP Profile

XACML-NRP Authorisation Interoperability profile for Network Resource Provisioning

- Part of the Phosphorus Project deliverable D.4.3.1 - "GAAA toolkit pluggable components and XACML policy profile for ONRP“ http://www.ist-phosphorus.eu/files/deliverables/Phosphorus-deliverable-D4.3.1.pdf
- Incorporates and extends XACML-Grid profile https://edms.cern.ch/document/929867/1
  - Developed as EGEE-OSG-Globus cooperation and implemented in the Globus and gLite middleware
- Attribute identifiers and attribute identification
  - URL-style and registered namespace http://authz-interop.org/nrp/xacml
    - Both XACML-Grid and XACML-NRP
  - SAML/XACML style – Attribute identifiers are attributes to more generic attribute names
- Supports topology related attributes and allows topology aware policy definition (e.g. policy definition use cases 5 and 6)
  - 3 topology description formats reviewed
    - Phosphorus Harmony/NSP (XML based) – *Currently supported and implemented*
    - OSCARS (2008) (XML based)
    - NDL by UvA (RDF based)
    - Prospectively will support OGF NML topology description format
    - Contributed as a usecase ton NML-WG

Basic use cases for policy definition in NRP

General access control:

- Use case 1: "User A is only allowed to use user endpoints X, Y and Z"
  - Defined as TNA (Transport Network Address)
- Use case 2: "User A is only allowed to use endpoints in domain N and M“

Access stage:

- Use case 3: “User/Group A is only allowed to invoke method/action X, Y, and Z”
- Use case 4: “User/Group A is only allowed to invoke method X,Y, and Z based on session delegation”
  - Including interdomain access and delegation

Reservation stage:

- Use case 5: “Apply {topology restrictions} to the path reservation in the next domain”
- Use case 6: “Check/match {topology/path restrictions} from the previous domain”

Conditional policy decision:

- Use case 8: “Allow conditional policy decisions using Policy Obligations and enforce policy decision conditions when evaluating authorisation request containing {Policy Obligations}”
  - Supported with XACML Policy Obligations and Obligations Handling Reference Model (OHRM) proposed as part of GAAA-NRP

XACML Policy and Request/Response format

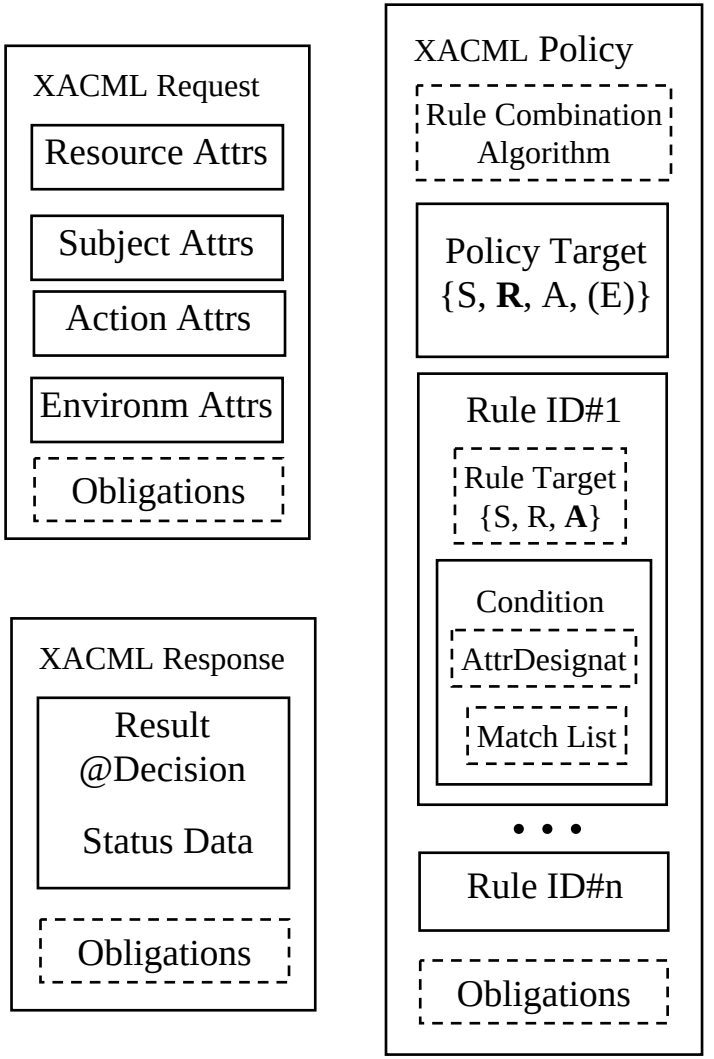
XACML standard specifies XACML policy format and XACML request/response messages

Policy consists of Policy Target and Rules

- Policy Target is defined for the tuple Subject-Resource-Action (-Environment)
- Policy Rule consists of Conditions and may contain Obligations
- Obligation defines actions to be taken by PEP on Policy decision by PDP

XACML PDP returns all Obligations that match policy decision (defined by attribute “FulfillOn”) from both PolicySet and comprising individual policies

XACML specification and implementation doesn’t support any functionality related to attributes validation and Obligations handling



Example - Resource related attributes

Attribute name	Attribute ID	Full XACML attributeId semantics (ns-prefix = http://authz-interop.org/nrp/xacml)
Domain ID	domain-id	{ns-prefix} /resource/domain-id
Subdomain	subdomain	{ns-prefix} /resource/sub-domain
VLAN	vlan	{ns-prefix} /resource/vlan
TNA	tna (+ tna-prefix)	{ns-prefix} /resource/tna-prefix/tna
Node	node	{ns-prefix} /resource/node
Link	link-id	{ns-prefix} /resource/link-id
avrDelay	delay	{ns-prefix} /resource/delay
maxBW	bandwidth-max	{ns-prefix} /resource/bandwidth
Resource type	resource-type	{ns-prefix} /resource/resource-type ({ns-prefix} /resource/device)
Resource federation	federation	{ns-prefix} /resource/federation

- Describes topology related information
- 3 topology description formats were reviewed
- Phosphorus NSP/WP1 topology description
- NDL by UvA
- OSCARS (currently used)
- Link parameters: average delay and maximum bandwidth
- ReservationEPR that may directly or indirectly define the resource federation or security/ administrative domain
- Federation that defines a number of domains or nodes sharing common policy and attributes

Example – Topology/Path information in the ResourceContent of the XACML Request

```
<xacml-context:Resource><xacml-context:ResourceContent>
<ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">dummy</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">1171</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">
          Virtual dummy domain</ns3:Description>
  <ns3:ReservationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyReservation/services/MyService</ns3:ReservationEPR>
  <ns3:TopologyEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyTopology/services/MyService</ns3:TopologyEPR>
  <ns3:NotificationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyNotification/services/MyService</ns3:NotificationEPR>
  <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">128.0.0.0/16</ns3:TNAPrefix>
  <ns3:avgDelay xmlns:ns3="http://ist_phosphorus.eu/nsp">50</ns3:avgDelay>
  <ns3:maxBW xmlns:ns3="http://ist_phosphorus.eu/nsp">1111</ns3:maxBW>
 </ns4:Domains>
</xacml-context:ResourceContent></xacml-context:Resource>
```

XPath expression

xacml:RequestContextPath="./xacml-context:Resource/xacml-context:ResourceContent/
xacml-context:Attribute/xacml-context:AttributetValue/ns4:Domains/ns3:avgDelay"

Example - XACML Policy Rule to match ResourceContent

```
<Rule RuleId="urn:oasis:names:tc:xacml:2.0:scas-policy:example001:rule" Effect="Permit">
    <Target/>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-than">
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">100</AttributeValue>
     </Apply>
     <AttributeSelector RequestContextPath="RequestContextPath=
          "./xacml-context:Resource/xacml-context:Attribute/xacml-context:AttributetValue/
                ns4:Domains/ns3:avgDelay"
          MustBePresent="true" DataType="http://www.w3.org/2001/XMLSchema#integer"/>
    </Condition>
</Rule>
```

XACML-NRP Policy Obligations

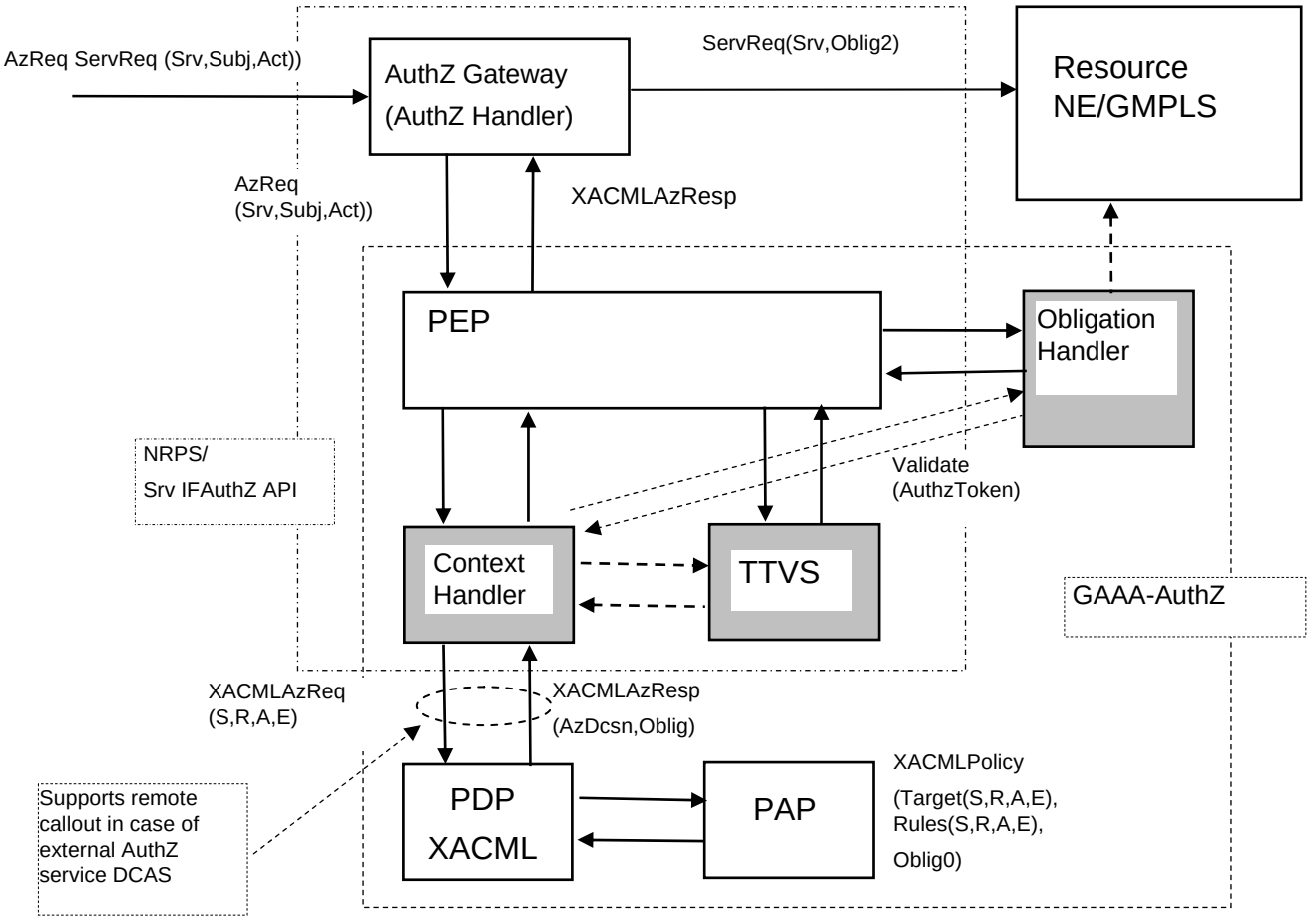
Suggested policy obligations for multidomain NRP

- General conditional policy decisions
- Intra-domain network/VLAN mapping for cross-domain connections
  - Can be used to map external/interdomain border links/endpoints to internal VLAN and sub-network
- Account mapping and delegation (inter/cross-domain)
- Type of service (or QoS) assigned to a specific request or policy decision
- Quota assignment
- Service combination with implied conditions (e.g., computing and storage resources)
- Usable resources e.g. number of access/view, volume of traffic, etc
  - *Advance Resource Reservation (ARR) type – Fixed, Deferrable, Malleable*

GAAA-NRP implementation – GAAA-TK Java library

- GAAA-TK pluggable Java library provides reference implementation of the GAAA-NRP framework
- GAAA-TK library provides all necessary AuthZ mechanisms and service components to support AuthZ sessions context and Obligations handling
  - AuthZ ticket format for extended interdomain AuthZ session management
  - Supports Pilot token based Interdomain signalling and access control with Access tokens
  - Can be used and ensure signalling and access control transparency at all Networking layers (Service, Control and Data planes)
- XACML-NRP profile is implemented *as* configurable metadata/constants set (XML metadata file and Java constants)
  - Supports also XACML-Grid profile
- Integrated into the Phosphorus project Network Service Plane (NSP Harmony) test-bed and uses simple XACML policy model
- Allows integration with other AuthZ frameworks (Grid and network middleware)
  - Supports Unicore6 Explicit Trust Delegation SAML Assertions
- Recent Version 0.8 is available from http://staff.science.uva.nl/~demch/projects/aaauthreach/index.html

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

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

- Main and Security services life-cycle management
  - Consistent security at each of the composition, deployment, operation stages
- SLA negotiation and support in XACML-NRP
- Virtualisation and platform security bootstraping
  - Using TCPA and TPM enabled platforms
- 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?
- 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

Expected to be partly answered by studying ITU-T documents of the X, M, Y groups

Looking for existing frameworks/experiences (1)

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

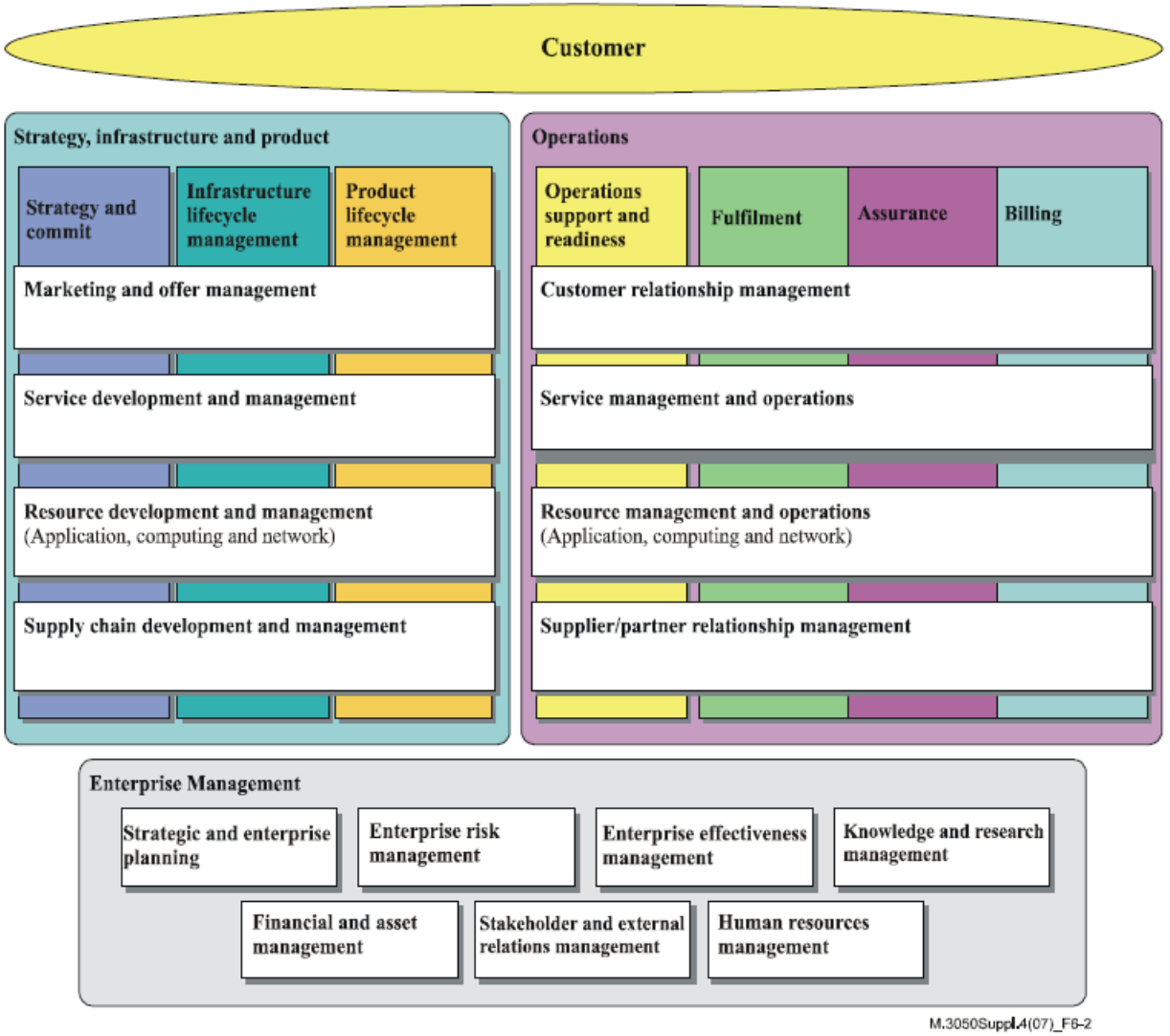
- ITU-T standards
  - M: Telecommunication management, including TMN and network maintenance (including M.3050 eTOM framework)
  - X: Data networks, open system communications and security
  - Y: Global information infrastructure, Internet protocol aspects and next-generation networks
- TMF standardised 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
- OASIS SOA and security related standards
  - Service Components Architecture (SCA) management
    - Including SCA-BPEL, SCA
  - nn
- IETF
  - Review and re-factor COPS (Common Open Policy Service) framework for new Geysers technology platform

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



Defines Business Process Framework for TeleManagement network operators

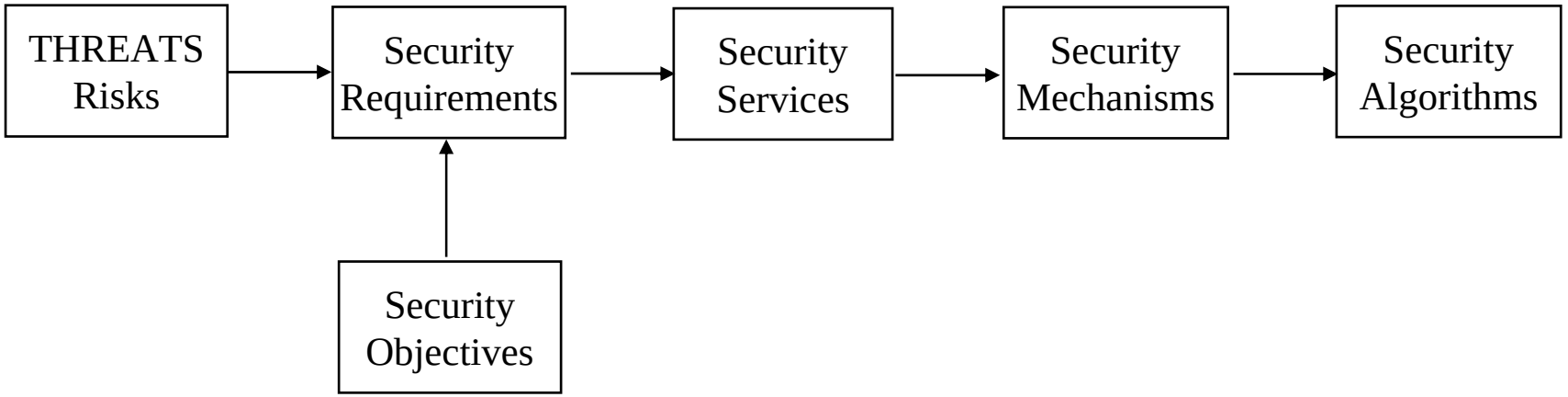
T-REC M.3050.0-M.3050.4

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 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)

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

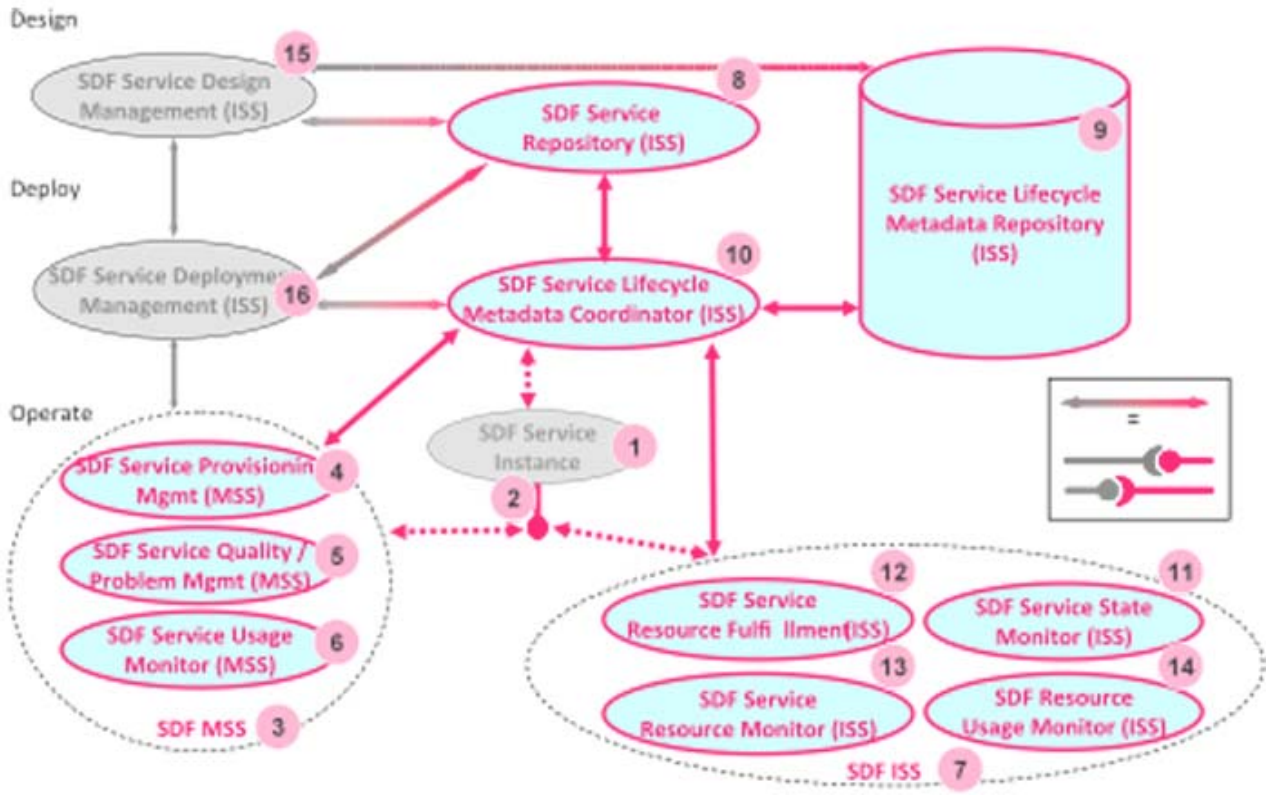
- NGOSS - New Generation Operations Systems and Software principles (http://www.tmforum.org/BestPracticesStandards/ServiceDeliveryFramework/4664/Home.html)
  - Separation of Business Process from Component Implementation
  - Loosely Coupled Distributed System
  - Shared Information Model
  - Common Communications 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 - Service
2 - Service Management Interface
3 - Management Support Service (SDF MSS)
4 - Service Provisioning Management
5 - Service Quality/Problem Management
6 - Service Usage Monitor
7 - Infrastructure Support Service
8 - Service Repository
9 - Service Lifecycle Metadata Repository
10 - Service Lifecycle Metadata Coordinator
11 - Service State Monitor
12 - Service Resource Fulfillment
13 - Service Resource Monitor
14 - Resource Usage Monitor
15 - Service Design Management
16 - Service Deployment Management

Suggested future research and developments

- 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

- TVS functionality

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

TVS functionality – Access Control and Signalling

Basic TVS functionality is checking validity of an access token received from the PEP or AuthZ gateway/service

- Extended TVS functionality allow token re-building when processing request from the previous domain and relaying to the next domain
  - Special method to Validate&Relay pilot tokens
- Additionally, TVS may be used for token security context distribution, e.g. token key(s), at the reservation stage or at the stage of the reserved resource deployment

TVS supports pilot tokens signalling during the reservation stage

- Can be used for building dynamic security association of the reserved resources

TVS is implemented as a component and a profile of the GAAA Toolkit GAAAPI package

- Can be integrated into the target network provisioning systems and applications, in particular OSCARS and DRAGON (result of cooperation with Internet2)

The current token handling model uses shared secret HMAC-SHA1 algorithm:

```
TokenKey = HMAC(GRI, tb_secret)
TokenValue = HMAC(GRI, DomainId, TokenId, TokenKey)
```

where GRI – global reservation identifier

tb_secret – shared Token Builder secret.