Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning

Yuri Demchenko
System and Network Engineering Group
University of Amsterdam

CPSRT 2010 Workshop
2 December 2010
CloudCom2010 Conference
30 October - 3 December 2010, Indianapolis
Outline

- Background for this research
- On-Demand Infrastructure Services Provisioning and Composable Services Architecture (CSA)
  - CSA Service Delivery Framework and Services Lifecycle Management
- Proposed Security Services Lifecycle Management and related security mechanisms
- Implementation – GAAA Toolkit and Security sessions management
- Summary and Discussion
Background to this research

- **Current projects**
  - GEANT3 JRA3 Composable Services
    - European NREN infrastructure
  - GEYSERS – On-demand Optical + IT infrastructure resources provisioning
    - Wide participation from large European network (Telefonika, Alcatel-Lucent, Interoute) and application providers (SAP)

- **Past projects**
  - EGEE Grid Security middleware – gLite Java Authorisation Framework
  - Phosphorus project Security architecture for multi-domain Network Resource Provisioning
    - GAAA-NRP and XACML-NRP profile
    - Multidomain Network Resource Provisioning (NRP) model and workflow
Use Case – e-Science infrastructure

Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure

Initial effort to build – estimated 2 Yrs
Outsource to current telco provider – approx. 2 months
Target with new business model – 2 hrs

User A
User K
User P

Visualisation
Visualisation

Instrument (Manufactoring)

Grid Center
Grid Center

Grid Storage T0
Grid Storage T1

Computing Cloud

Cloud Storage

Control & Monitoring

Permanent link
High Speed link provisioned on demand
Link provisioned on-demand
Components of the typical e-Science infrastructure involving multidomain and multi-tier Grid and Cloud resources and network infrastructure

On-demand infrastructure services provisioning environment
- Security along the whole provisioning process and service/infrastructure lifecycle
- Manageable/user controlled security
- Securing remote executing environment
- Security context/session management

Permanent link
High Speed link provisioned on demand
Link provisioned on-demand
GEYSERS Reference Model for Infrastructure Virtualisation

Roles:
- VIO – Virtual Infrastructure Operator
- VIP - Virtual Infrastructure Provider
- PIP - Physical Infrastructure Provider
Security Service Lifecycle Management in On-Demand Resources/Services Provisioning

- On-Demand Infrastructure Services Provisioning requires definition of Services Lifecycle Management
  - Multidomain multi-provider environment
  - Includes standard virtualisation procedures and mechanisms
- Requires dynamic creation of Security/Trust Federations in multi-domain environment
  - Based on available Trust Anchors
    - Physical Resources (hosting platforms)
    - SLA or SLA negotiators/contractors
    - All other security context/credentials/keys should be derived from them
- Access control infrastructure dynamically created and policy/attributes dynamically configured
  - Access/authorisation session/context management

- Composable Services Architecture (CSA) as a platform for dynamically configurable composable services provisioning
Composable Services Architecture

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

Separation of Data Plane, Control Plane, Management Plane
CSA Services Delivery Framework (SDF)
Composable Services Provisioning Workflow

Main stages/phases
- Service Request (including SLA negotiation)
- Composition/Reservation (aka design)
- Deployment, including Registration/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)

*Based on the TMF SDF*
Goal: Automation of the whole service delivery and operation process

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

Design

- SDF Service Design Management (ISS)
- SDF Service Repository (ISS)
- SDF Service Lifecycle Metadata Coordination (ISS)
- SDF Service Design Management (ISS)

Deploy

- SDF Service Deployment Management (ISS)
- SDF Service Lifecycle Metadata Repository (ISS)
- SDF Service Resource Monitor (ISS)
- SDF Service State Monitor (ISS)
- SDF Service Resource Fulfillment (ISS)
- SDF Service Resource Usage Monitor (ISS)
- SDF Service Usage Monitor (ISS)

Operate

- SDF Service Provisioning Management (MSS)
- SDF Service Quality/Problem Management (MSS)
- SDF Service Usage Management (MSS)

1 – Service Instance
2 - Service Management Interface
3 – Service Functional Interface
4 - Management Support Service (SDF MSS)
8 - Infrastructure Support Service (ISS)
10 - Service Repository
16 - Service Design Management

DESIGN stage
9 - Service Repository
10 - Service Lifecycle Metadata Repository
17 - Service Deployment Management

DEPLOYMENT stage
11 - Service Lifecycle Metadata Coordinator

OPERATION stage
5 - Service Provisioning Management
12 - Service State Monitor
13 - Service Resource Fulfillment
14 - Service Resource Monitor
15 - Resource Usage Monitor

Composite Services provisioned on-demand

SDF MSS
SDF ISS
Composable Services Architecture – Lifecycle stages workflow

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

MD SLC – Service Lifecycle Metadata
GEMBus – GEANT Multidomain Bus

Applications and User Terminals
Composable Services Middleware (GEMBus/GE SB)
Logical Abstraction Layer for Component Services and Resources

Control & Management Plane (Operation, Orchestration)
Proxy (adaptors/containers) – Composed/Virtualised Services and Resources
Proxy (adaptors/containers) – Component Services and Resources

Storage Resources
Compute Resources
Network Infrastructure
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 SecuritySLM and general SLM

Additional 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 (as part of Planning stage) that provides support for complex reservation process including required access control and policy enforcement.

**Registration & Synchronisation** stage (as part Deployment stage) 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.
Relation between SSLM/SLM stages and supporting general and security mechanisms

<table>
<thead>
<tr>
<th>SLM stages</th>
<th>Request</th>
<th>Design/Reservation Development</th>
<th>Deployment</th>
<th>Operation</th>
<th>Decommissioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process/Activity</td>
<td>SLA Negotiation</td>
<td>Service/Resource Composition Reservation</td>
<td>Composition Configuration</td>
<td>Orchestration/Session Management</td>
<td>Logoff Accounting</td>
</tr>
</tbody>
</table>

Mechanisms/Methods

<table>
<thead>
<tr>
<th>SLA</th>
<th>Workflow</th>
<th>Metadata</th>
<th>Dynamic Security Associatn</th>
<th>AuthZ Session Context</th>
<th>Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>(V)</td>
<td>V</td>
<td>(V)</td>
<td>V</td>
<td>(V)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>
Implementation suggestions

Extend existing GAAA-Toolkit pluggable Java library to support dynamic Security/AII infrastructure creation and integration with provisioned VI
  - Provides GAAA Authorisation API (GAAAPI) functions with extended AuthZ and session management functionality
Support for SDF workflow and Security Services Lifecycle Management
  - Needs general infrastructure services such as Metadata SLM
Define and implement Common Security Service Interface (CSSI)
  - Supports both internal applications calls and Web service integration via Spring security
  - Implements GSS-API and extends it with GAAAPI functionality
Use standard Messaging, Transport and Network security mechanisms provided by implementation platform
  - Implementation platform selection – ESB/WS/SOA (Fuse, Apache ServiceMix, etc.)
Multidomain Network/Complex Resource Provisioning (NRP/CRP) – Provisioning sequences

NRPS – Network Resource Provisioning System
NSP – Network Service Plain
DC – Domain Controller
IDC – Interdomain Controller

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

Token based policy enforcement
GRI – Global Reservation ID
AuthZ tickets for multidomain context mgnt
T - Token

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service
KGS – Key Generation Service
Multidomain Complex Resource Provisioning (CRP) – Stage 1 – Path building and Advance Reservation

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

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
Multidomain Complex Resource Provisioning (CRP) – Stage 2 – Deployment (setup and key distribution)

- **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

**Token based signalling and access control**
- **GRI** – Global Reservation ID
- **AzTicket** – AuthZ ticket for multidomain context mgnt
- **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
Multidomain Complex Resource Provisioning (CRP) – 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

**Abbreviations:**
- 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
CRP 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
Access Token and Pilot Token Types

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

**AType 1** – Access token containing Obligations collected from previous domains

**PType 0** – Container for GRI only

**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’ context may include the previous token and the domain’s trust anchor or public key

**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
XML Token Format – Access and Pilot Tokens

- Support inter-domain security/session context communication to allow multidomain provisioning scenarios
- Ensure Integrity of the AuthZ decision
  - Keeps AuthN/AuthZ context
  - Allow Obligated Decisions (e.g. XACML Obligations)
- Supports simple delegation scenarios
- Can be used for establish session-based trust relations between domains
- Allows easy mapping to SAML and XACML related elements
Chaining Pilot Tokens in multidomain signalling

* Pilot Token type 3 issued by domain UVA

```
<AAA:AuthzToken xmlns:AAA="http://www.aaauthreach.org/ns/AAA"
    Issuer=http://testbed.ist-phosphorus.eu/UVA/AAA/TVS/tokenpilot
    SessionId="740b241e711ece3b128c97f990c282adcbf476bb"
    TokenId="dc58b505f9690692f7a6312912d0fb4c" type="pilot-type3">
<AAA:TokenValue>190a3c1554a500e912ea75a367c822c09eceaa2f</AAA:TokenValue>
<AAA:DomainsContext>
    <AAA:Domain domainId="http://testbed.ist-phosphorus.eu/viola">
                        SessionId="2515ab7803a86397f3d60c670d199010a96cb51"
                        TokenId="c44a2f5f70346f6dc2a2244febcdd244">
            <AAA:TokenValue>dee1c29719b9098b361cab4cfcd086700ca2f414</AAA:TokenValue>
        </AAA:AuthzToken>
        <AAA:KeyInfo>http://testbed.ist-phosphorus.eu/viola/_public_key_</AAA:KeyInfo>
    </AAA:Domain>
</AAA:DomainsContext>
<AAA:AuthzToken>
```

Requestor ➔ Domain1 “viola” ➔ Domain2 “uva” ➔ Domain3 “uclp” ➔ Resource
Future work and Discussion

- Definition of and reference implementation of the Common Security Services Interface (CSSI)
  - As extension to industry adopted GSS-API
  - Incorporate GAAA-AuthZ (RFC2904) Authorisation interface
  - Extends for Session Security Context Management and dynamic trust/security association management

- Wide range of formalisation and modeling work

- Implementation in projects GEANT3 and GEYSERS

- CSA and Security Services Lifecycle Management model is proposed as a possible deliverable for OGF ISOD RG
Additional Information

- TMF SDF Lifecycle Management model
AuthN/AuthZ Infrastructure (AAI) in GEYSERS

Basic CSSI services:
- Data encryption
- Digital signature
- Authentication
- Authorization
- Policy management
- Security session and context management

Called from services (or part of core interfaces):
- SLI (SML-LICL)
- CCI (NCP-LICL)
- NLI (NCP-LICL)
- LPI (LICL-PHY)
- NIPS-UNI

GEYSERS Security (AAI)
GEYSERS AAI Reference Model

AAI Gateway
Common Security Services Interface (CSSI)

- AuthN Service
- PEP
- SecCtx Handler
- Token Validation Service (TVS)
- PDP
- PAP
- Dyn AC Service Mngnt
- Config, Attr, Trust/Key Mngnt

PEP: Policy Enforcement Point
PDP: Policy Decision Point
PAP: Policy Administration Point
DACS: Dynamic Access Control Service
GEMBus Infrastructure for Composable Service

GEMBus Infrastructure Services

GEMBus Component Services

Service 1 (CSrvID, SesID)
Service 2 (CSrvID, SesID)
Service 3 (CSrvID, SesID)
Service 4 (CSrvID, SesID)

ESB

GEMBus Messaging Infrastructure (GMI)

Routing
Configuration
Interceptors (AspOrient)

GMI 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
GEYSERS Reference Model

Role:
- VIO
- VIP
- PIP
Role of GEYSERS actors with respect to its architectural layers
GEYSERS Service Delivery Framework (SDF)

- **Service provisioning workflow by VIP:**
  - Creation of the Virtual Infrastructure (VI)
  - May include more engineers support

- **Service provisioning workflow by VIO:**
  - Creation and operation of the Virtual Infrastructure on-demand for specific project, tasks or user groups
  - Should be completely automatic

- Should also include activities/stages for infrastructure re-planning, restoration and migration

- Adopted TeleManagement Forum Service Delivery Framework (TMF SDF)

- GEYSERS Project - http://www.geysers.eu/
GEYSSERS Service Delivery Framework/Workflow

Geysers SDF supports both Geysers infrastructure development and deployments and its operation for on-demand Infrastructure services provisioning by VIO.

Service Request/SLA Negotiation
Planning (Design)
Deployment (Instant& Config&Synchro)
Operation &Monitoring (by VIO)
Decommissioning

Service Provisioning Workflow by VIO

Recovery/Migration
Re-planning

Network+IT Services Provisioning Workflow by VIO

Service Request/SLA Negotiation
Planning (Compos/Reserv)
Deployment
Registr&Synchro
Operation (Monitoring)
Decommissioning

Recovery/Migration
Re-planning
Existing framework in on-Demand Infrastructure Services Provisioning and Lifecycle Management

**TMF standardised frameworks, practices and procedures**
- SDF - Service Delivery Framework
- SLA management
- NGOSS – New Generation Operations System Services (including eTOM)

**Microsoft Security Development Lifecycle (SDL) Framework**
- Primarily focused on the product development process by engineers/programmers

SDF main stages and phases

Main stages/phases
- Service Request (including SLA negotiation)
- Planning (including Composition, Reservation and 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 should be supported by the Service Lifecycle Metadata Service (SL MD)