Control Plane security
Authorization across domains.

Cees de Laat

SURFnet

BSIK

EU

University of Amsterdam

SARA

TNO

NCF

Net
IRTF - AAAARCH - RG

Authentication Authorisation
Accounting ARCHitecture RG

chairs:
C. de Laat and J. Vollbrecht

www.aaaarch.org

RFC 2903, 2904, 2905, 2906, 3334
Basic AAA

- **Service perspective:**
  - Who is it who wants to use my resource
    » Establish security context
  - Do I allow him to access my resource
    » Create a capability / ticket /authorization
  - Can I track the usage of the resource
    » Based on type of request (policy) track the usage

- **User perspective**
  - Where do I find this or that service
  - What am I allowed to do
  - What do I need to do to get authorization
  - What does it cost

- **Intermediaries perspective**
  - Service creation
  - Brokerage / portals

- **Organizational perspective**
  - What do I allow my people to do
  - Contractual relationships (SLA’s)
The need for AAA

End user

Kingdom N

Remote service

Kingdom N+1

AAA

BB

management

RAA

BB

management

$$$
Multi domain case
Simple service access

Pitlochry, Scotland - Summer 2005
Use AAA concept to split (time consuming) service authorization process from service access using secure tokens in order to allow fast service access.
1. User (on Node1) requests a path via web to the WS.
2. WS sends the XML requests to the AAA server.
3. AAA server calculates a hashed index number and submits a request to the Scheduler.
4. Scheduler checks the SCHEDULE and add new entry.
5. Scheduler confirms the reservation to the AAA.
6. AAA server updates the POLICY_TABLE.
   6a. AAA server issues an encrypted key to the WS.
   6b. AAA server passes the same key to the PEP.
7a. WS passes the key to the user.
    7b. AAA server interacts with PEP to update the local POLICY_TABLE on the PEP.
8. User constructs the RSVP message with extra Token data by using the key and sends to VLSR-1.
9. VLSR-1 queries PEP whether the Token in the RSVP message is valid.
10. PEP checks in the local POLICY_TABLE and return YES.
11. When VLSR-1 receives YES from PEP, it forwards the RSVP message.
12. All nodes process RSVP message (forwarding/response)
13. The Ethernet switches are configured
14. LSP is set up and traffic can flow
Grid Application

RB-A

NRM-A
CRM-A
SRM-A

Network-A

Grid Administrative Domain - A

RB-B

NRM-B
CRM-B
IRM-B

Network-B

Grid Administrative Domain - B

GLIF Grid Resource Registry

Resource Registry

RB: Resource Broker
DNRM: Domain Network Resource Manager
CRM: Compute Resource Manager
IRM: Instrument Resource Manager
SRM: Storage Resource Manager

GAI: Grid Application Interface
GNI: Grid Network Interface
GCI: Grid Compute Interface
GSI: Grid Storage Interface
GII: Grid Instrument Interface

Publish Resource Information
Publish/Subscribe Broker + Resource Information / References
Phosphorus

European Multi-Domain Test-Bed Including Phosphorus Planned Developments

- SARA
- Distributed Storage
- APIs & AAA
- GMPLS/G²MPLS
- UKLight
  Essex
  All Optical Test Bed
- CESNET
- GMPLS/G²MPLS
- DRAC
- Data Streaming
- APIs & AAA
- G-OUNI E-NNI
- G-OUNI E-NNI
- I2CAT
- UCLP
- APIs & AAA
- G-OUNI E-NNI
- E-NNI
- GEANT2
- GLIF
- APIs & AAA
- E-NNI G-OUNI
- GMPLS/G²MPLS
- PIONIER
- APIs & AAA
- GMPLS/G²MPLS
- WISDOM
- Distributed Storage
- APIs & AAA
- ARGON
- G-OUNI
- E-NNI
- GMPLS/G²MPLS
- KoDaVis
- APIs & AAA
- Distributed Storage
- Data Streaming
- Optical link
- Network - Network signalling
- User - network signalling