# IRTF - AAAARCH - RG

# Authentication Authorisation Accounting ARCHitecture RG

chairs:

C. de Laat and J. Vollbrecht

www.aaaarch.org

RFC 2903, 2904, 2905, 2906

# Contents of this talk

- This space is intentionally left blank

# History & Charter

- Authorization subgroup of AAA-WG
- Commonality in authorization space
- Tie in policy from all WG's
- IRTF-RG chartered in Dec 1999
  - This RG will work to define a next generation AAA architecture that incorporates a set of interconnected "generic" AAA servers and an application interface that allows Application Specific Modules access to AAA functions.

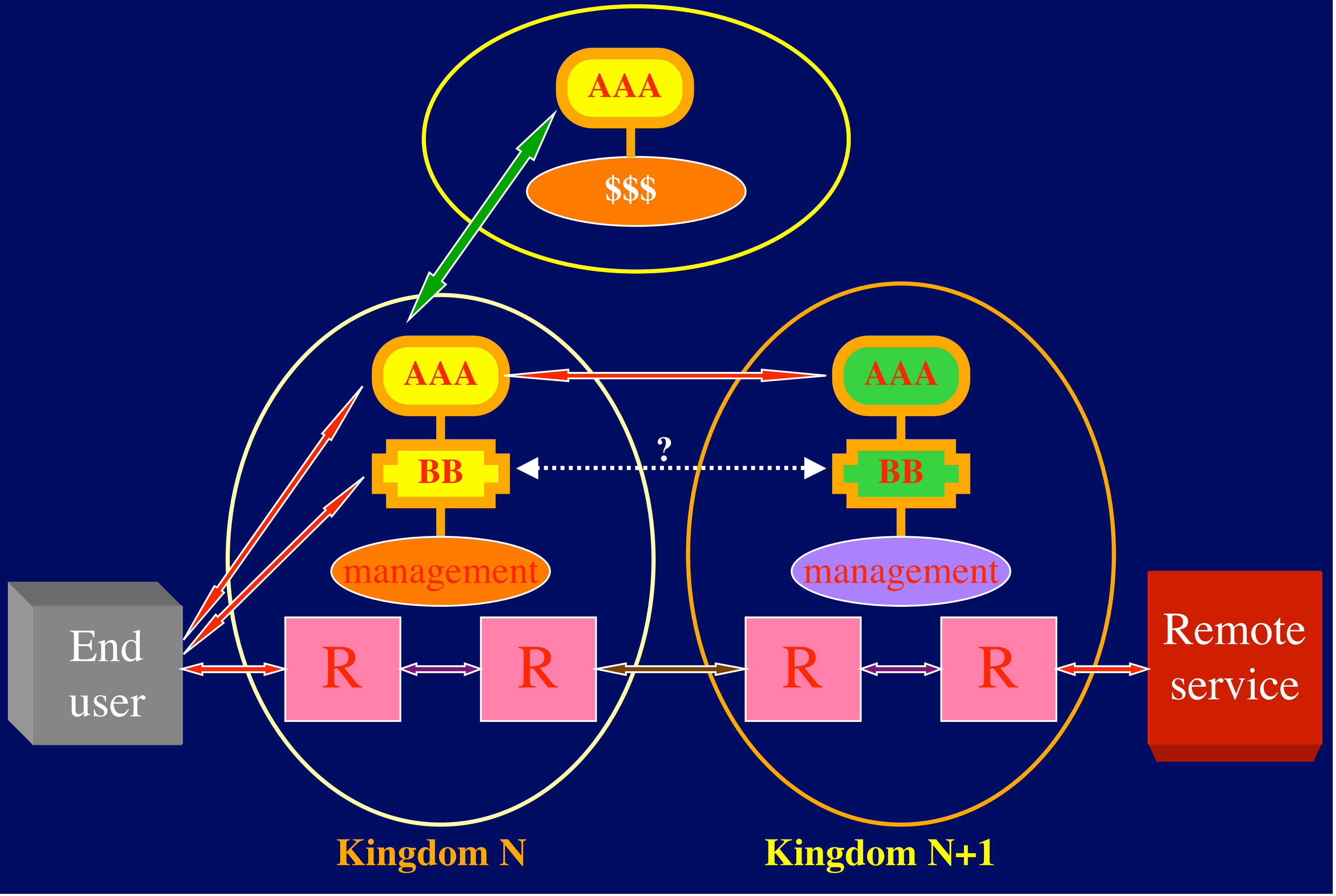
# From charter

- The architecture's focus is to support AAA services that:
  - can inter-operate across organizational boundaries
  - are extensible yet common across a wide variety of Internet services
  - enables a concept of an AAA transaction spanning many stakeholders
  - provides application independent session management mechanisms
  - contains strong security mechanisms that be tuned to local policies
  - is a scalable to the size of the global Internet

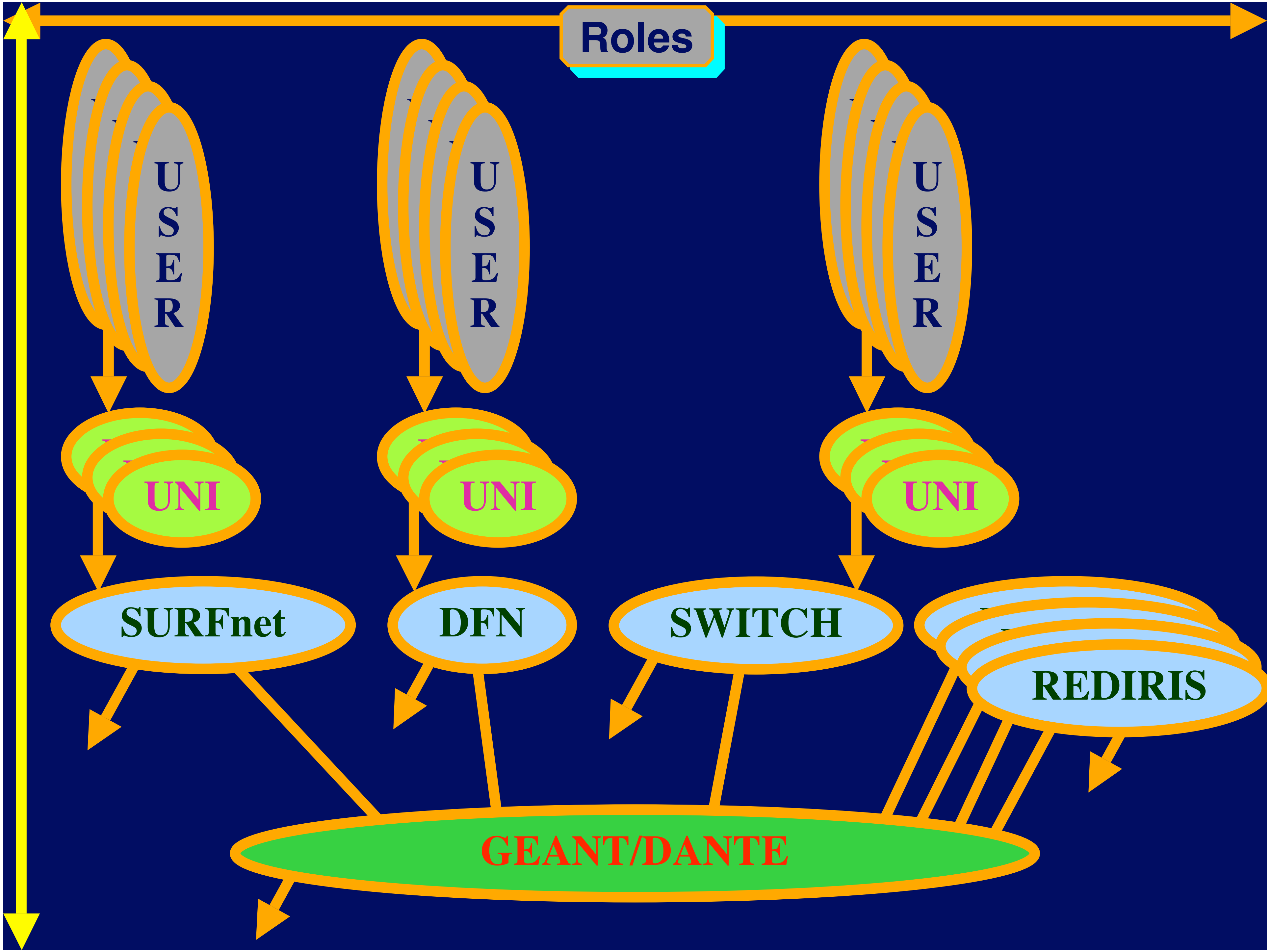
# Basic AAA

- 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



# Roles



USER

USER

USER

UNI

UNI

UNI

SURFnet

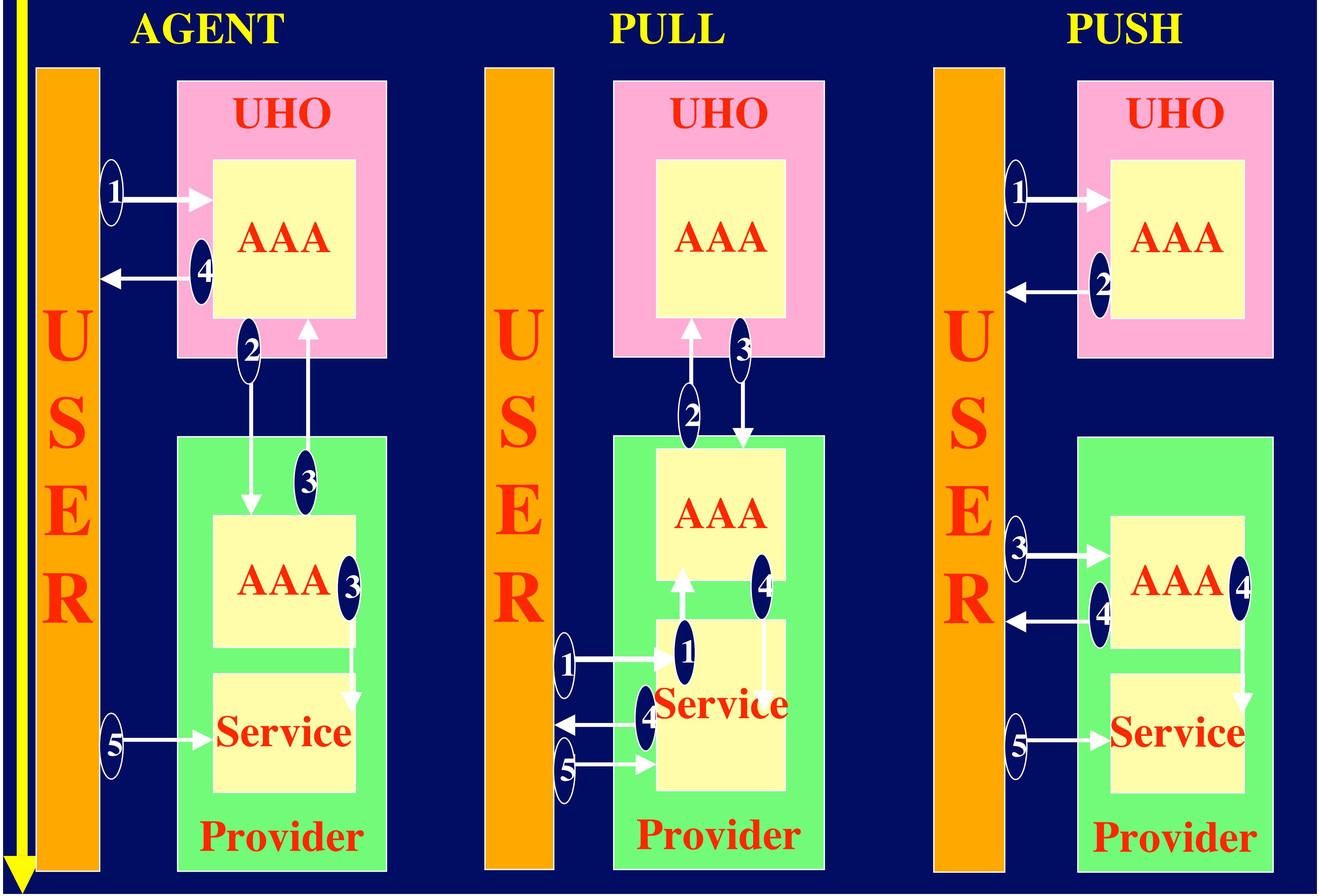
DFN

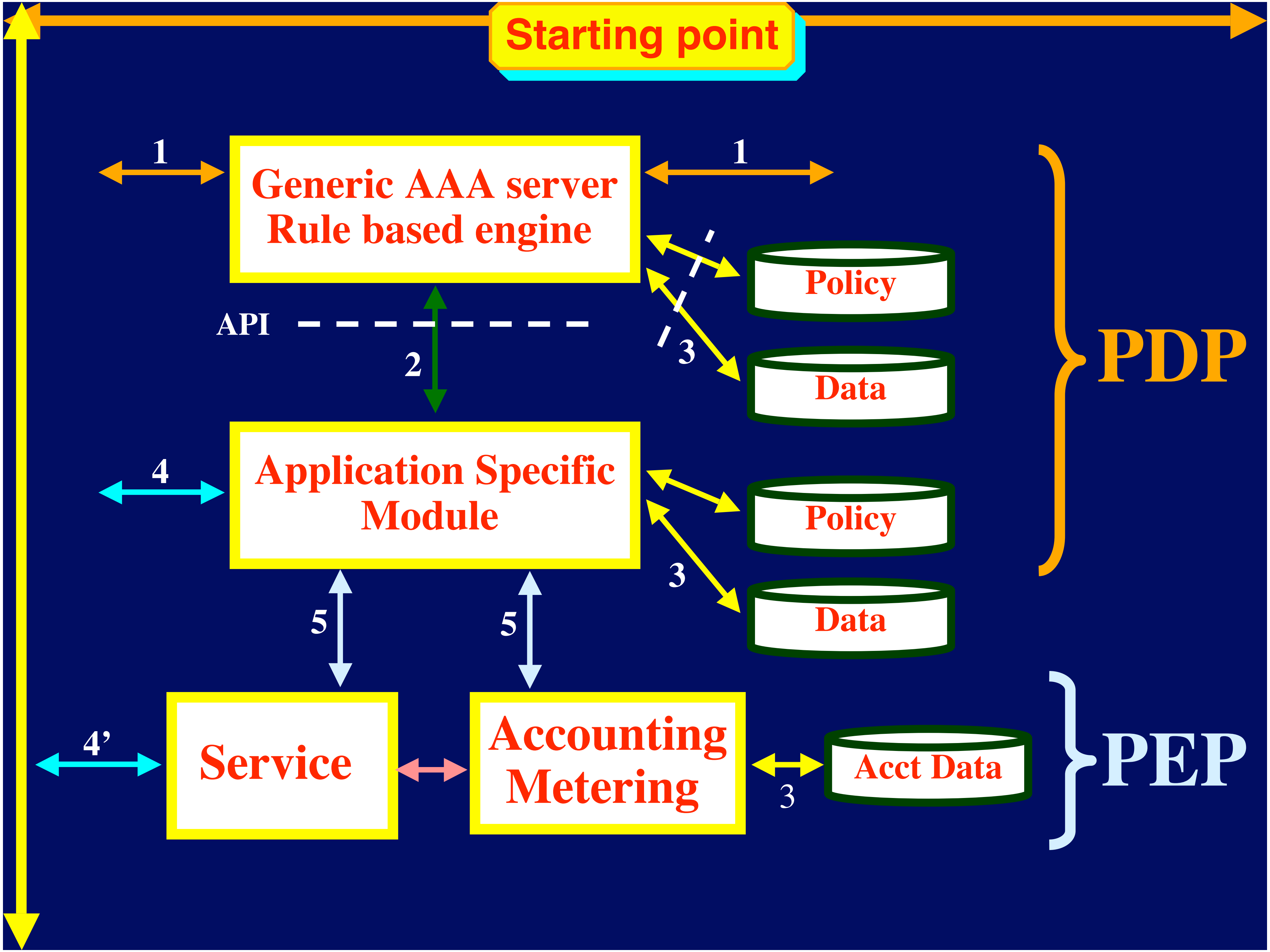
SWITCH

REDIRIS

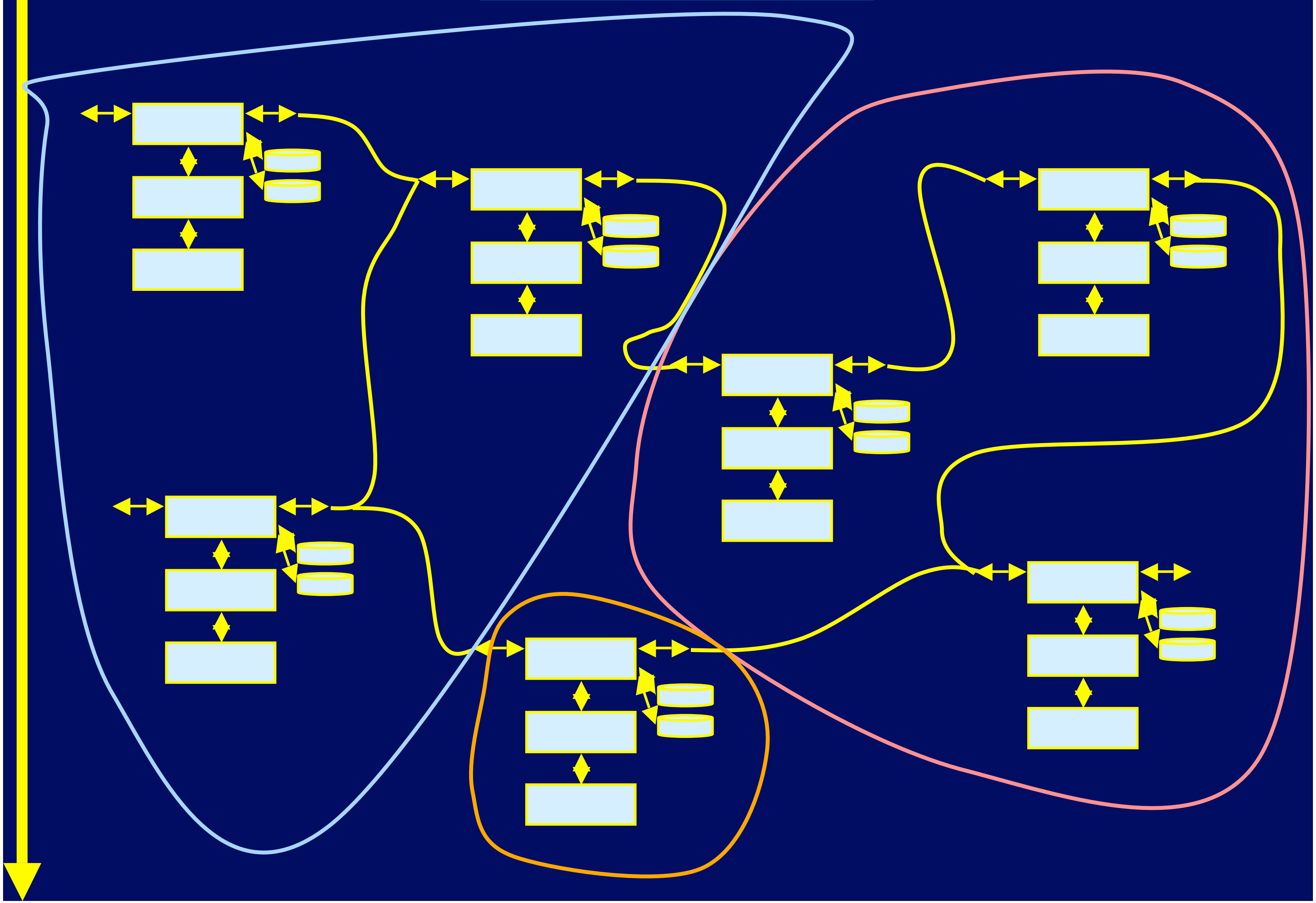
GEANT/DANTE

# Authorization Models




Starting point
1
Generic AAA server
Rule based engine
1
Policy
API
2
3
Data
PDP
4
Application Specific
Module
Policy
3
Data
5
5
4'
Service
Accounting
Metering
Acct Data
3
PEP

# Multi domain case



# Agenda 50th IETF

CHAIRS: Cees de Laat <delaat@science.uva.nl>
John Vollbrecht <jrv@interlinknetworks.com>

| | |
|---|---|
| Cees de Laat | Agenda bashing, FNT and opening remarks |
| Cees de Laat | draft-irtf-aaaarch-generic-struct-00.txt |
| John Vollbrecht | draft-irtf-aaaarch-session-id-00.txt |
| Sebastian Zander | draft-irtf-aaaarch-pol-acct-02.txt |
| Guus Sliepen | draft-irtf-aaaarch-aaa-pol-01.txt |
| Guus Sliepen | draft-taal-aaaarch-generic-pol-01.txt |
| Steven Tuecke | security in the grid, overview |
| Bob Morgan | Shibboleth update |
| Bob Morgan | OASIS security-services TC |
| Henk Jonkers | Accounting Examples |
| chairs | closing remarks, next steps, summary, collect pink sheets |

# Agenda 51th IETF

CHAIRS: John Vollbrecht < jrv@interlinknetworks.com >
Cees de Laat < delaat@science.uva.nl >

| | | |
|---|---|---|
| Cees de Laat | 10 | : Agenda bashing, FNT and opening remarks |
| Cees de Laat | 10 | : Status, drafts and ongoing activities |
| Christian Hesselman | 10 | : Content and QoS Policies in Multi-domain Heterogeneous Mobile Systems |
| Walter Weiss | 40 | : draft: draft-ietf-rap-access-bind-00.txt<br>title: "Framework for Binding Access Control to COPS Provisioning" |
| John Vollbrecht | 20 | : discussion: next steps AUTH-PIB<br>see memo on mailing list |
| Arie Taal | 29 | : draft: draft-irtf-aaaarch-generic-pol-00.txt<br>title: A grammar for Policies in a Generic AAA Environment |
| Guus Sliepen | 1 | : draft: draft-irtf-aaaarch-aaa-pol-01.txt<br>title: Policies in AAA |
| Bob Morgan | 15 | : Shibboleth and related projects update, impact of Globus |
| chairs | 15<br>===<br>150 | : closing remarks, next steps, summary, collect colored sheets |

# Opening remarks

- since San Diego:
  - interim meeting in Utrecht -> draft
  - 3 new drafts
  - 2 reworked
  - 2 teleconferences
    - About 8 participants
  - Discussion started with Grid-Forum
- Participation/contribution
  - Apart from about 3 or 4 places -> POOR!
- Evening meeting
- Re-charter (or not)

# Opening remarks

- since Minneapolis:
  - 1 new draft in AAAARCH, 1 (AUTH) in RAP
  - 1 AUTH related interim meeting in Utrecht
  - 0 reworked
  - 0 teleconferences in AAAARCH
  - About 10 teleconferences related to AUTH
- Participation/contribution
  - Apart from about 3 or 4 places -> POOR!
- Re-chartered

# Charter - research items

- develop generic AAA model by specifically including Authentication and Accounting UNDERWAY
- develop auditability framework specification that allows the AAA system functions to be checked in a multi-organization environment NJET
- develop a model for management of a "mesh" of interconnected AAA Servers NJET
- describe interdomain issues using generic model NJET
- define in a high level and abstract way the interfaces between the different components in the architecture UNDERWAY
- define distributed AAA related policy framework ON THE TABLE
- develop an accounting model that allows authorization to define the type of accounting processing required for each session ON THE TABLE
- implement a simulation model that allows experimentation with the proposed architecture UNDERWAY
- work with RAP-WG to develop an Authentication Information management model ON THE TABLE
- work with GRID-Forum to align the security and AAA architectural ideas UNDERWAY

# Current drafts

1. draft-irtf-aaaarch-aaa-pol-01.txt
   Title: Policy in AAA

2. draft-spence-aaaarch-objmsg-00.txt
   Title: Data Objects and Message Types in the Generic AAA Architecture

3. draft-irtf-aaaarch-session-id-00.txt
   Title: Session ID

4. draft-irtf-aaaarch-generic-struct-00.txt
   Title: Structure of a Generic AAA Server

5. draft-taal-aaaarch-generic-pol-01.txt (superceded by 6)
   Title: Policies in a Generic AAA Environment

6. draft-irtf-aaaarch-generic-policy-00.txt
   Title: A grammar for Policies in a Generic AAA Environment

7. draft-irtf-aaaarch-pol-acct-03.txt SUBMITTED FOR RFC
   Title: Policy-based Accounting

# Research Group - info

- Research Group Name: AAAARCH - RG
- Chair(s)
  - John Vollbrecht -- jrv@interlinknetworks.com
  - Cees de Laat -- delaat@science.uva.nl
- Web page
  - www.irtf.org
  - www.aaaarch.org
- Mailing list(s)
  - aaaarch@fokus.gmd.de
  - For subscription to the mailing list, send e-mail to

    majordomo@fokus.gmd.de with content of message

    subscribe aaaarch

    end
  - will be archived, retrieval with frames and in plain ascii:
    - » http://www.fokus.gmd.de/glone/research/aaaarch/
    - » http://www.fokus.gmd.de/glone/research/mail-archive/aaaarch-current
    - » ftp://ftp.fokus.gmd.de/pub/glone/mail-archive/aaaarch-current

AAAARCH