IRTF - AAAARCH - RG

Authentication Authorisation Accounting ARCHitecture RG

chairs:

C. de Laat and J. Vollbrecht

www.aaaarch.org

RFC 2903, 2904, 2905, 2906, 3334

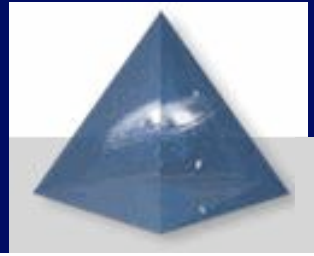
Contents of this talk

- This space is intentionally left blank

Except for:

EU IST-2001-32459

SURFnet



Faculty of Science

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

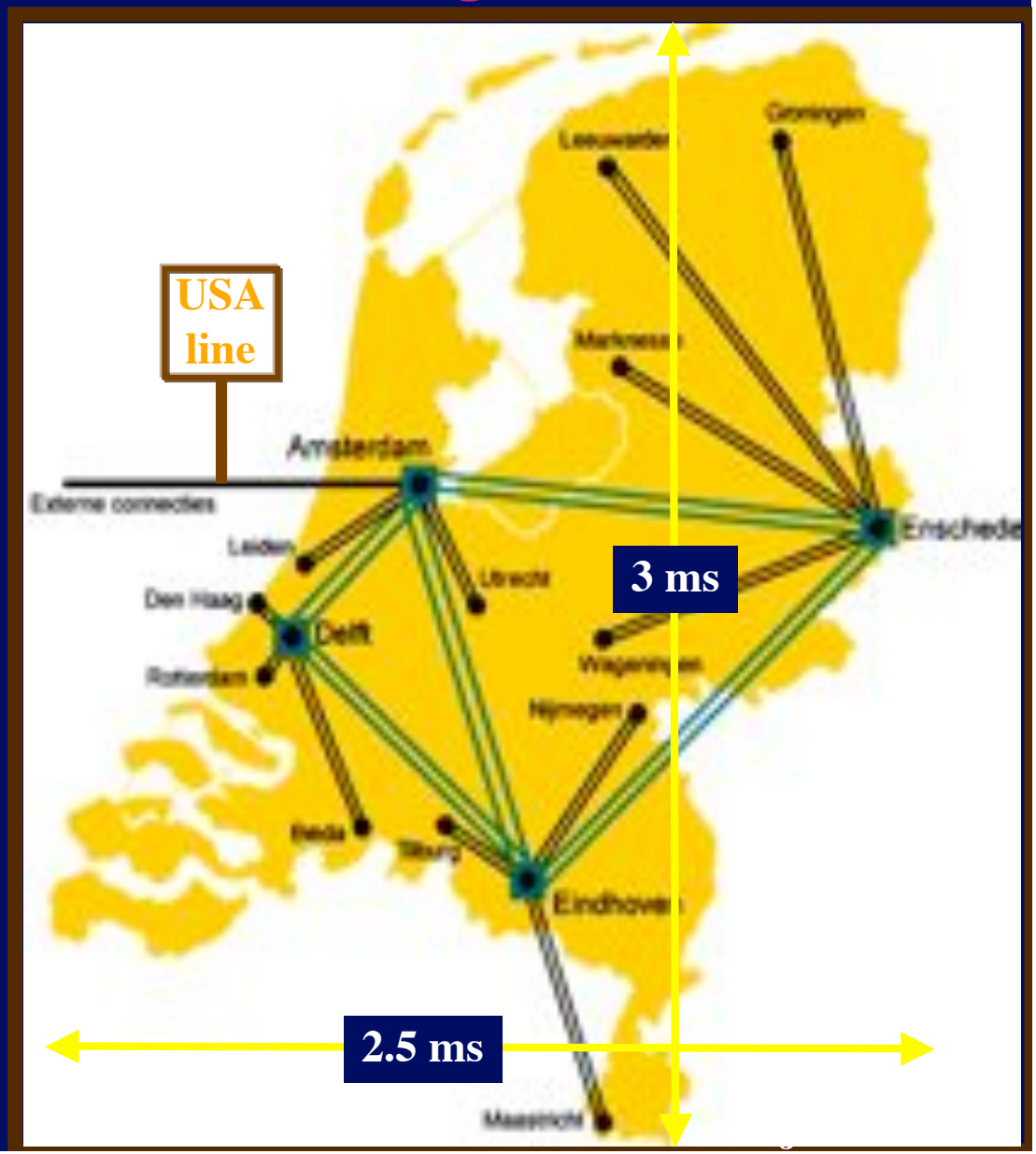
Basic AAA

- **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)

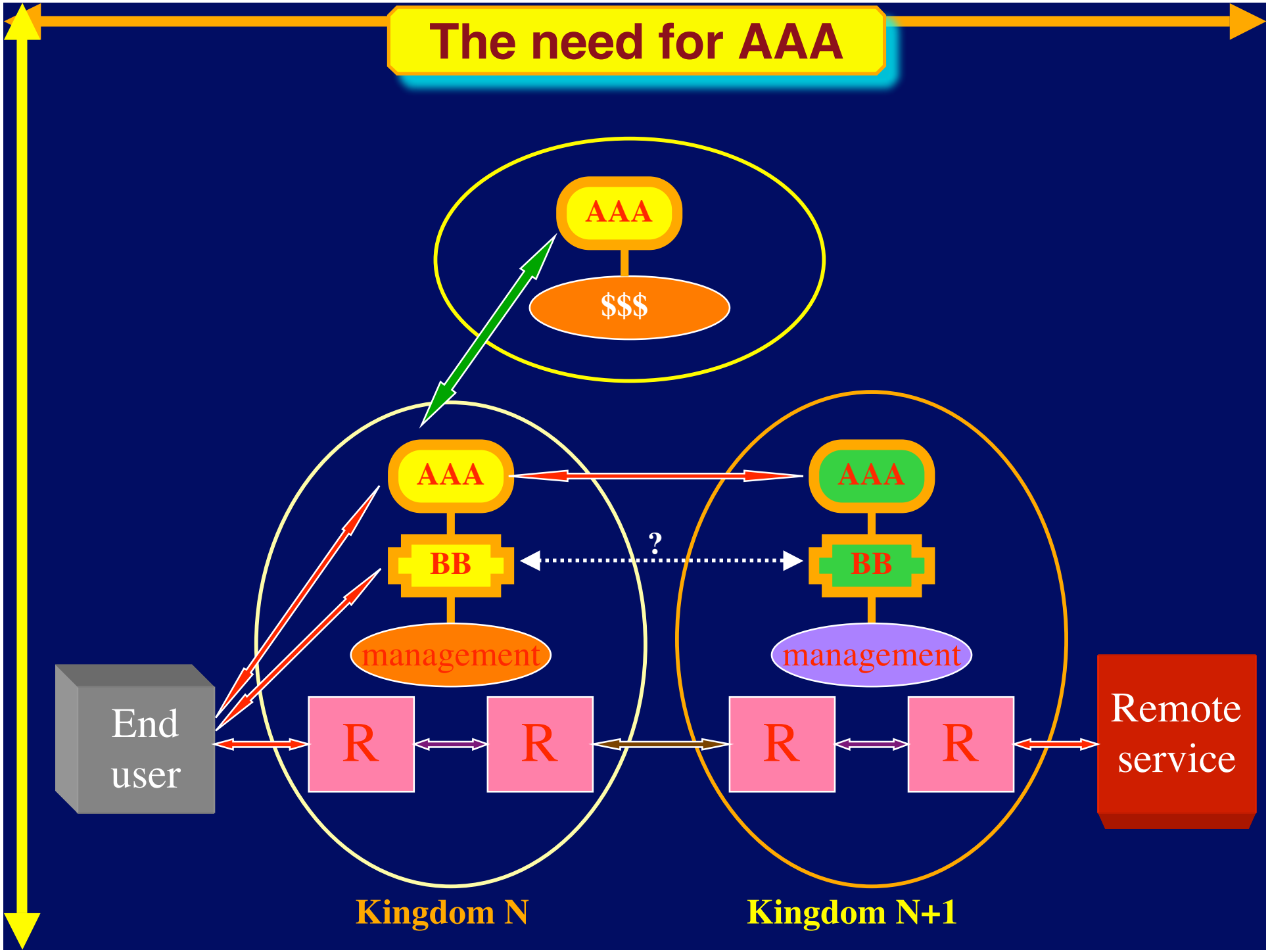
Multi Kingdom Problem

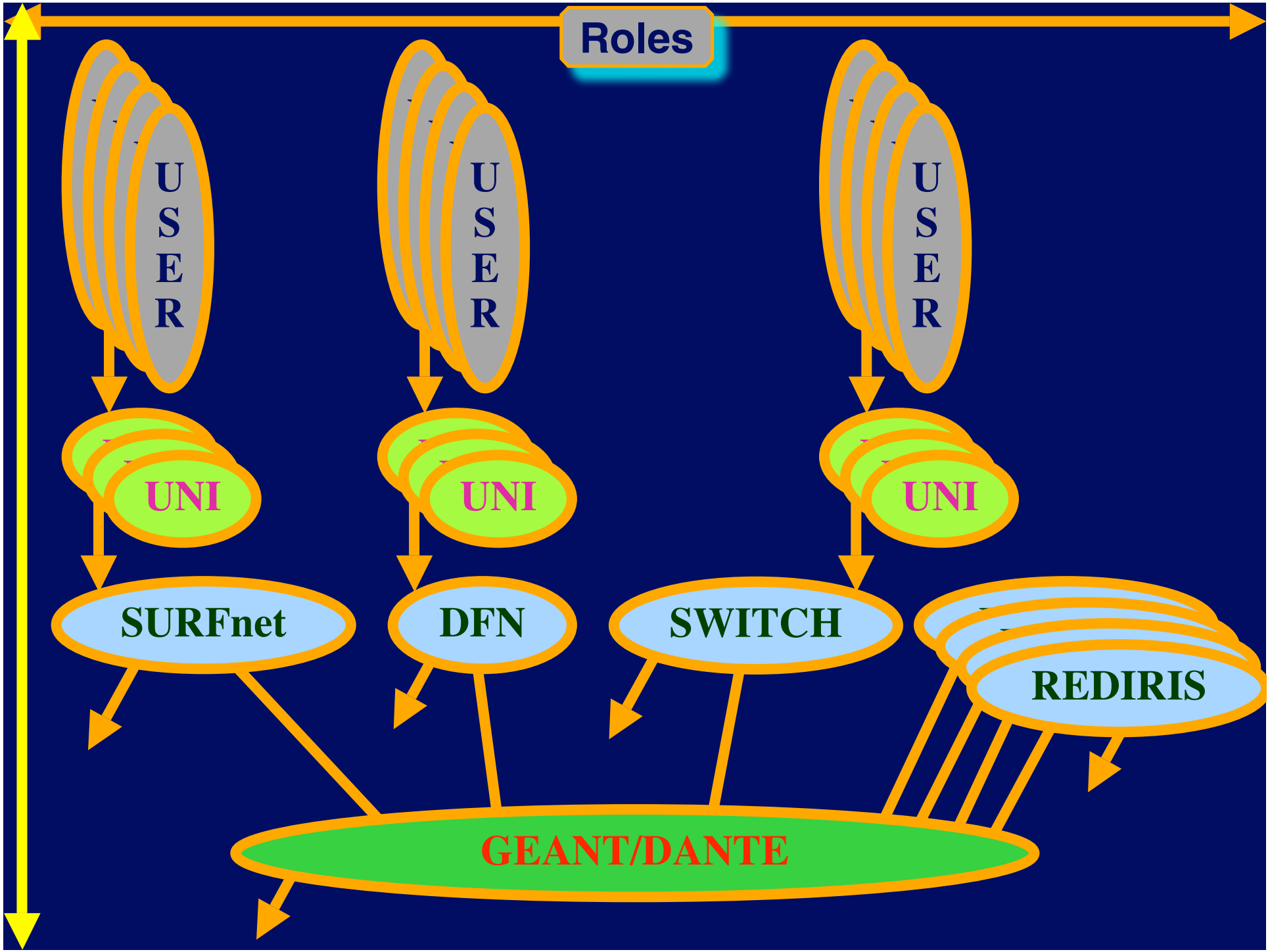
Physics-UU to IPP-FZJ => 7 kingdoms

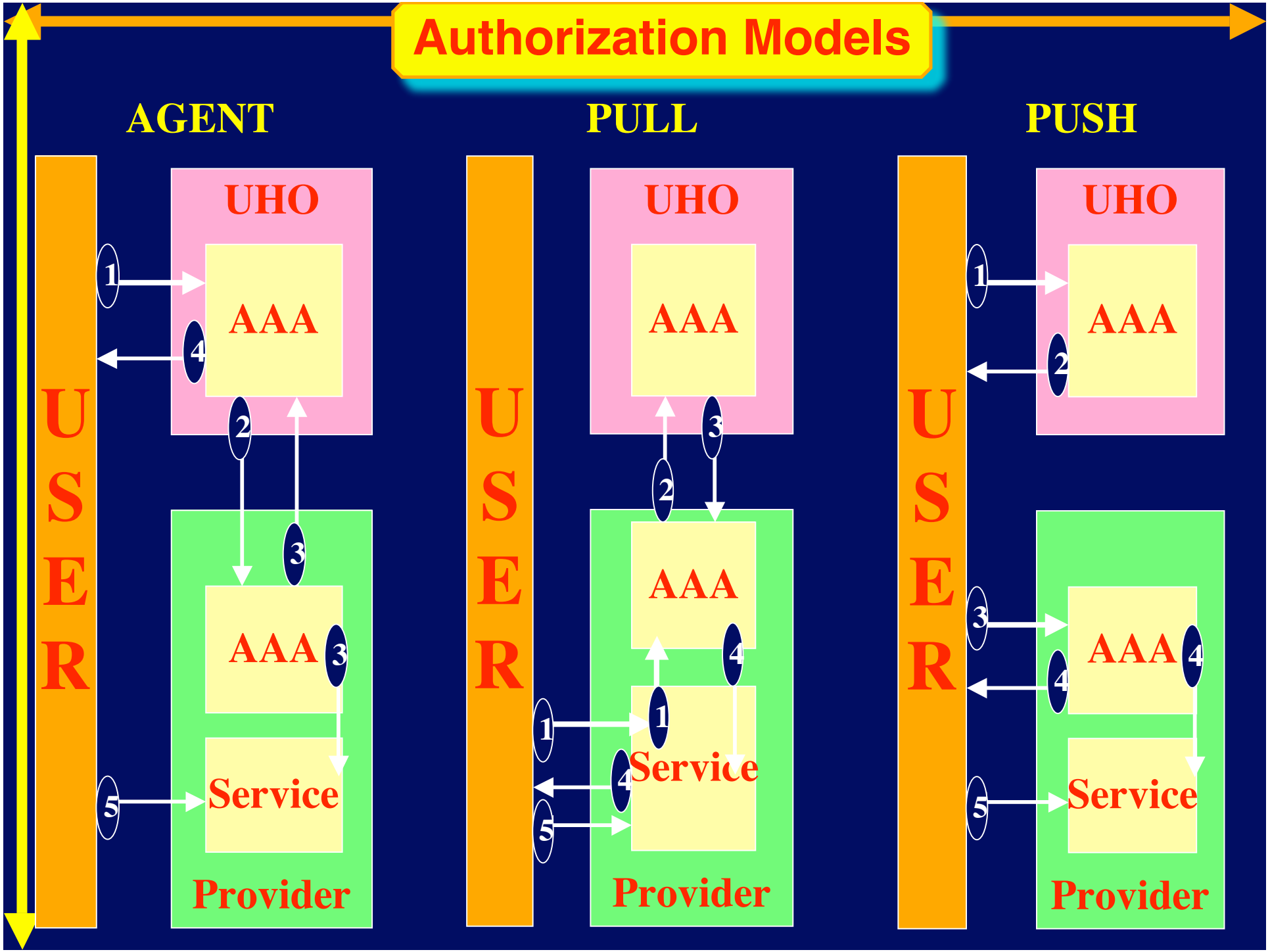
- Netherlands
  - » Physics dept
  - » Campus net
  - » SURFnet
- Europe
  - » TEN 155
- Germany
  - » WINS/DFN
  - » Juelich, Campus
  - » Plasma Physics dept

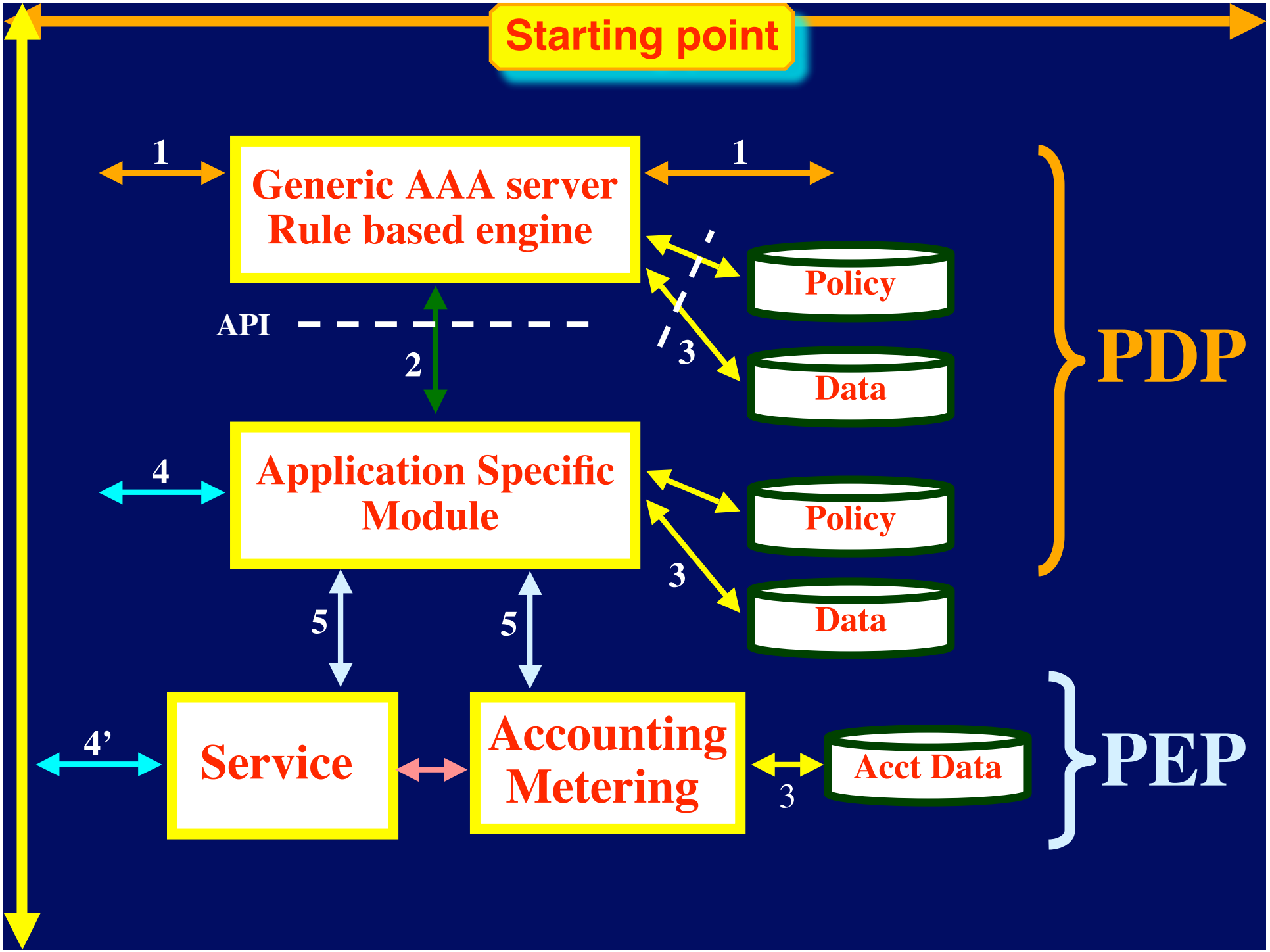


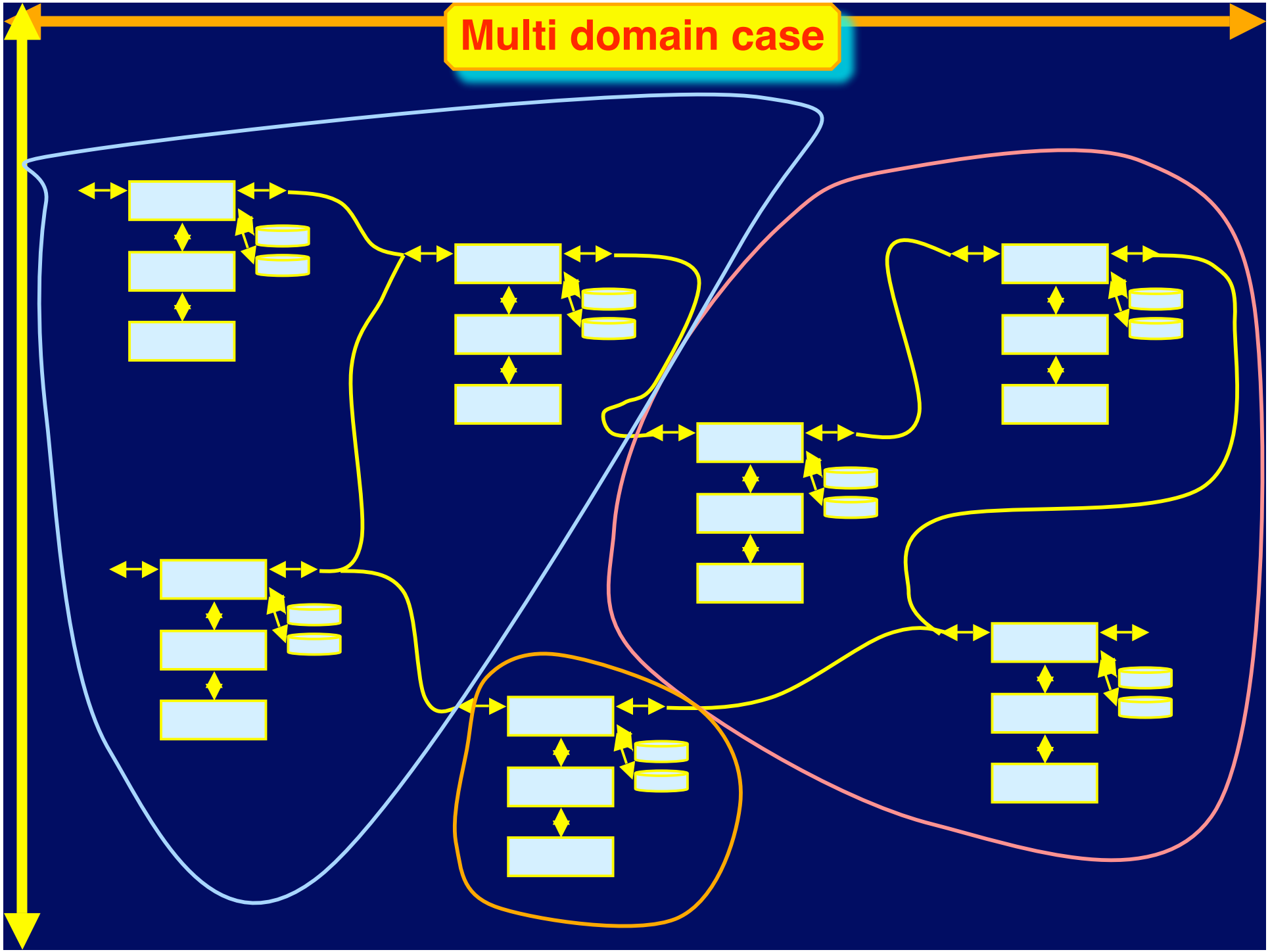
The need for AAA




Roles
USER
USER
USER
UNI
UNI
UNI
SURFnet
DFN
SWITCH
REDIRIS
GEANT/DANTE


Authorization Models
AGENT
PULL
PUSH
USER
UHO
AAA
Service
Provider
1
2
3
4
5


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
3
Acct Data
PEP


Multi domain case

Example BoD request

```
<AAARequest version="0.1" type="BoD">
 <AuthorizationData>
    <Credential type=”simple”>
       <ID>person1</ID>
       <Key>1#fdjkj9#esn34k</Key>
    </Credential>
 </AuthorizationData>
 <BodData>
       <Source>100.10.20.30</Source>
       <Destination>110.1.2.3</Destination>
       <Bandwidth>2500</Bandwidth>
       <StartTime>now</StartTime>
       <Duration>3600</Duration>
  </BodData>
</AAARequest>
```

Example of BoD driving Policy

```
if
(
   (
     ASM::Authorizer.authorize(
                Request::AuthorizationData.Credential.ID,
                Request::AuthorizationData.Credential.Key
                                  )
)
then
(
   ASM::RM.BoD(
                Request::ServiceData.SwitchData.Source,
                Request::ServiceData.SwitchData.Destination,
                Request::ServiceData.SwitchData.Bandwidth,
                Request::ServiceData.SwitchData.StartTime,
                Request::ServiceData.SwitchData.Duration
                   )
   ;
   Reply::Answer.Message = "Request successful"
)
else
(
   Reply::Error.Message = "Request failed"
)
```

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

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


AAARCH