Control Plane security

Authorization across domains.

Cees de Laat

SURFnet

BSIK

EU

University of Amsterdam

SARA

TNO

NCF

IRTF - AAAARCH - RG

Authentication Authorisation Accounting ARCHitecture RG

chairs:

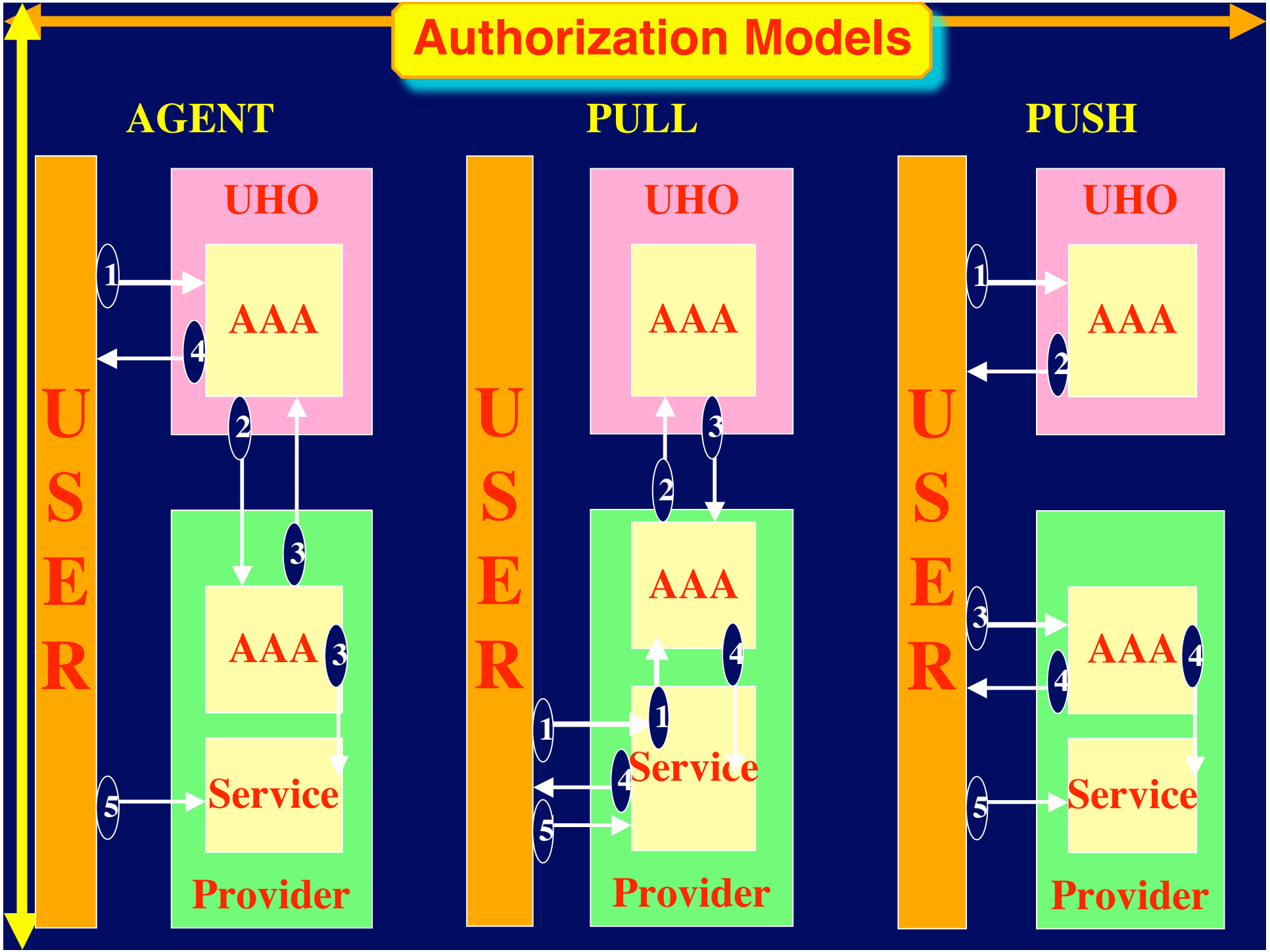
C. de Laat and J. Vollbrecht

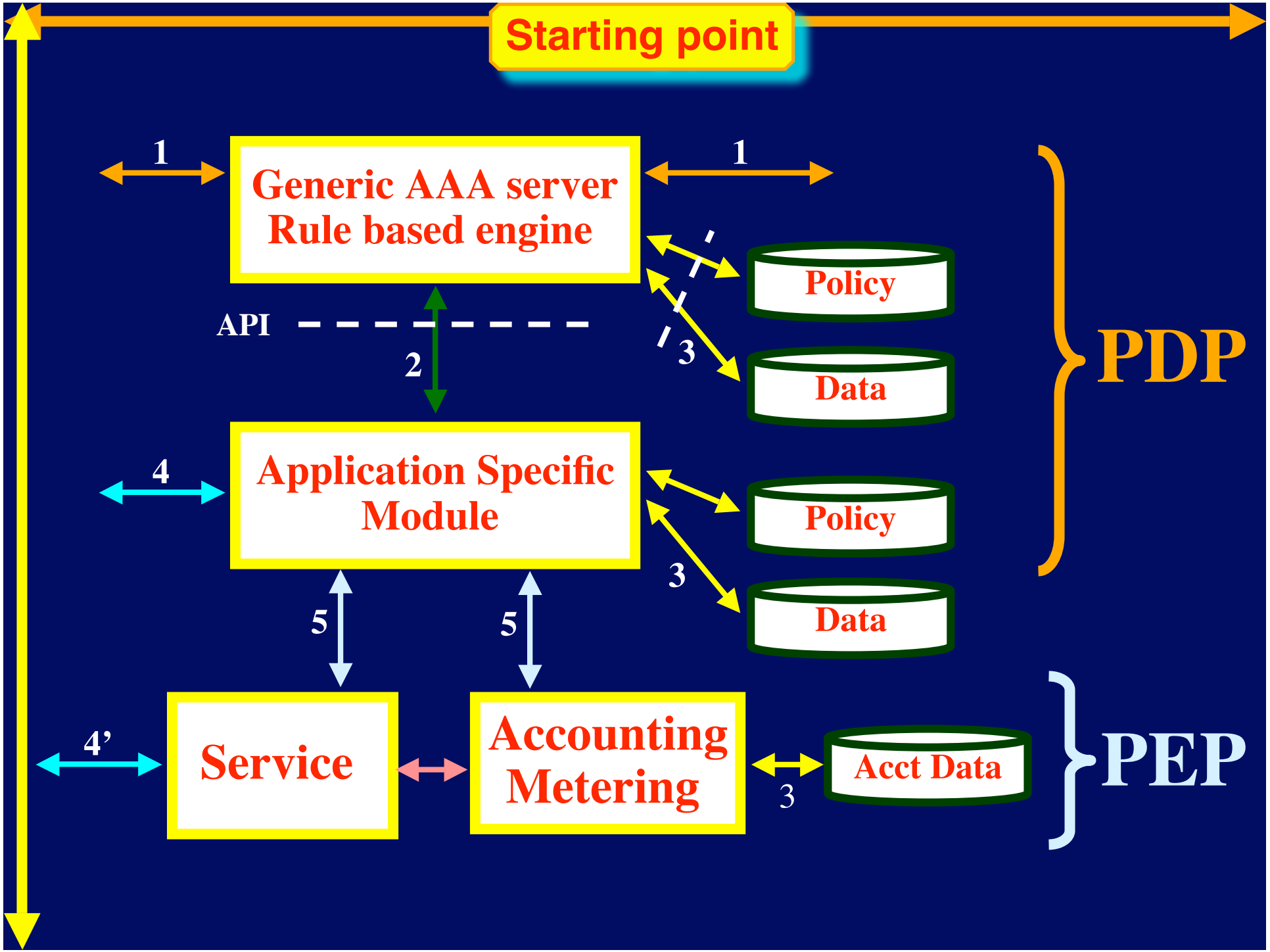
www.aaaarch.org

RFC 2903, 2904, 2905, 2906, 3334

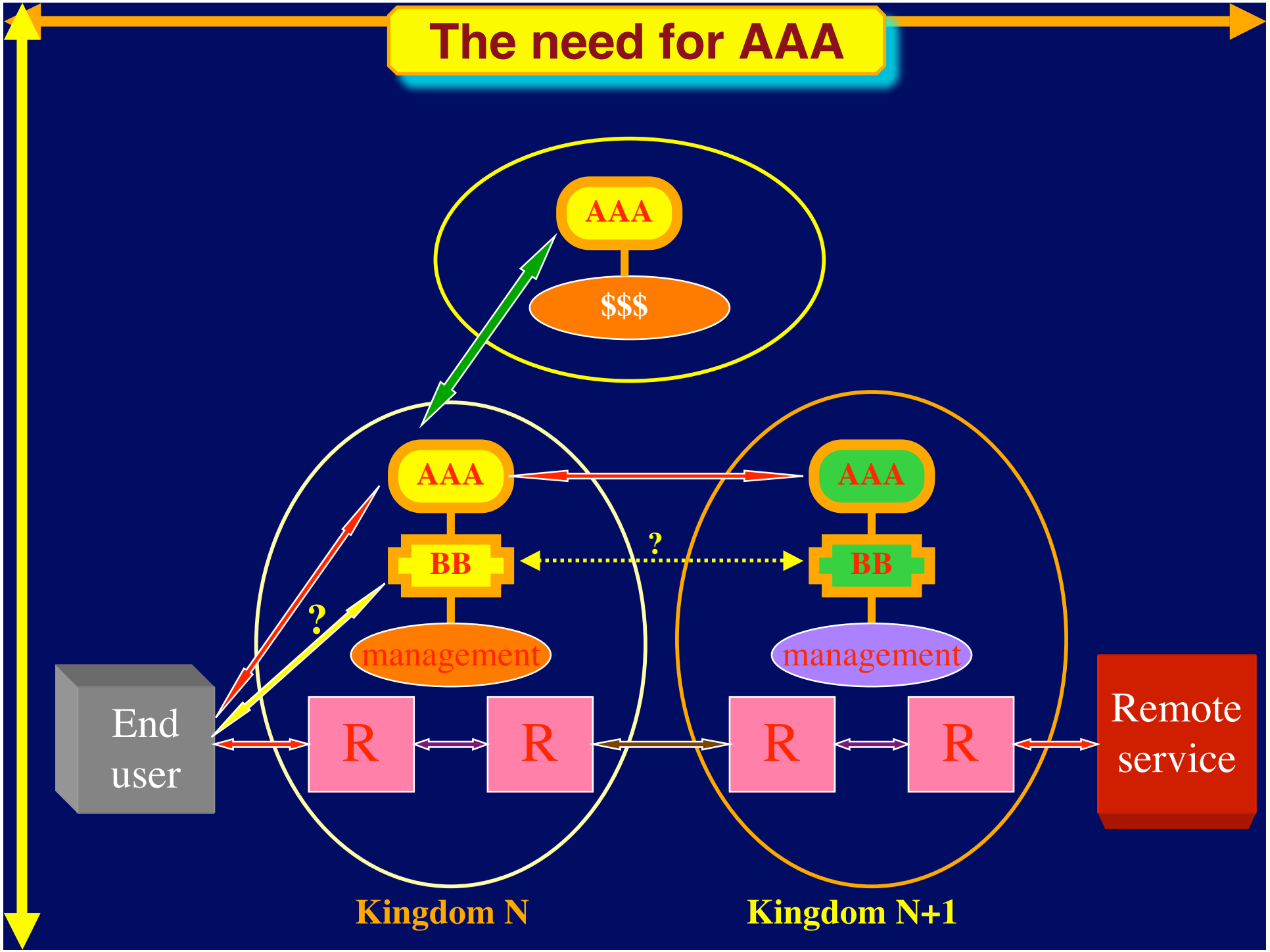
Basic AAA

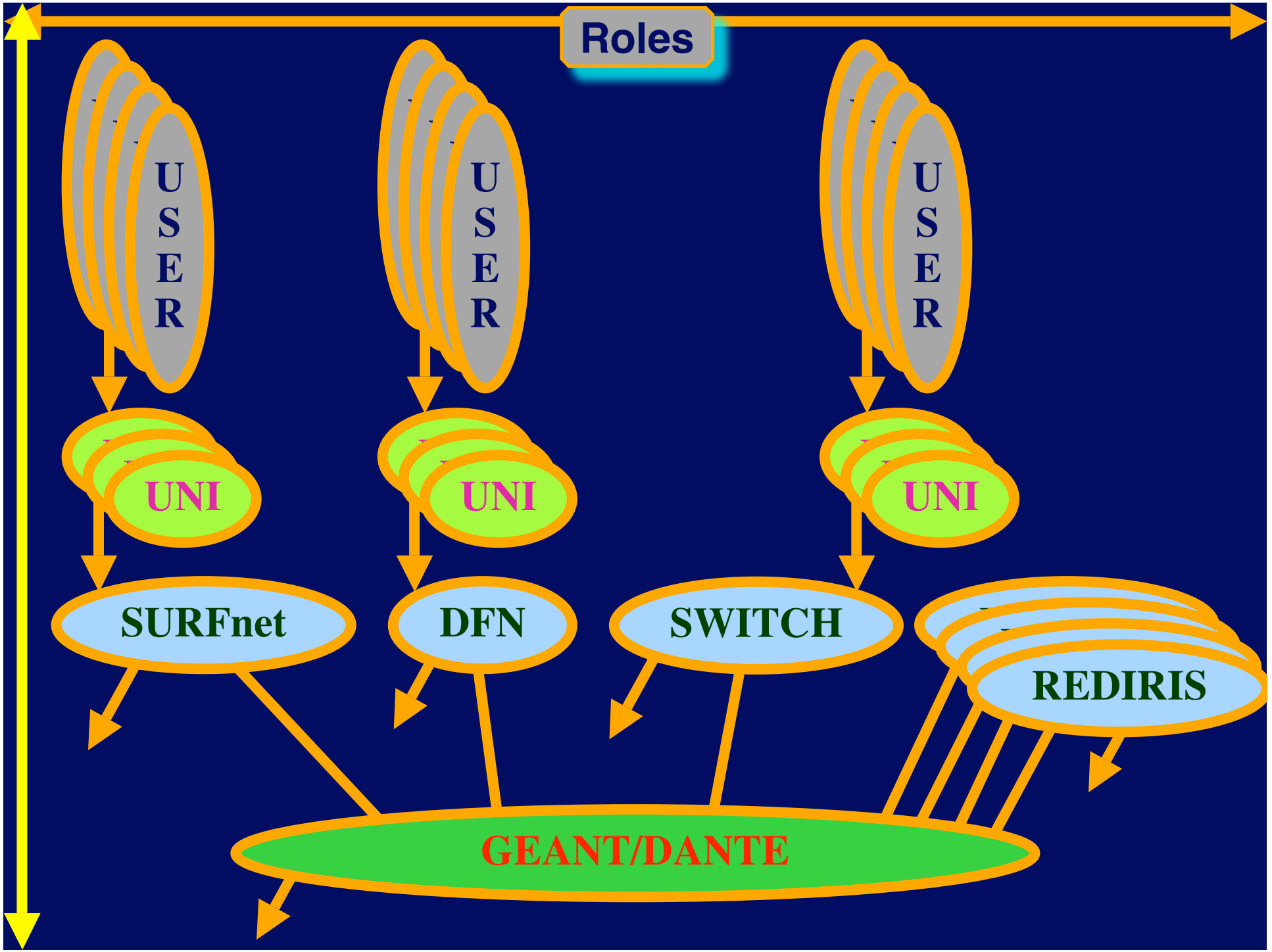
- **Service perspective:**
  - Who is it who wants to use my resource
    - » Establish security context
  - Do I allow him to access my resource
    - » Create a capability / ticket /authorization
  - Can I track the usage of the resource
    - » Based on type of request (policy) track the usage
- **User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

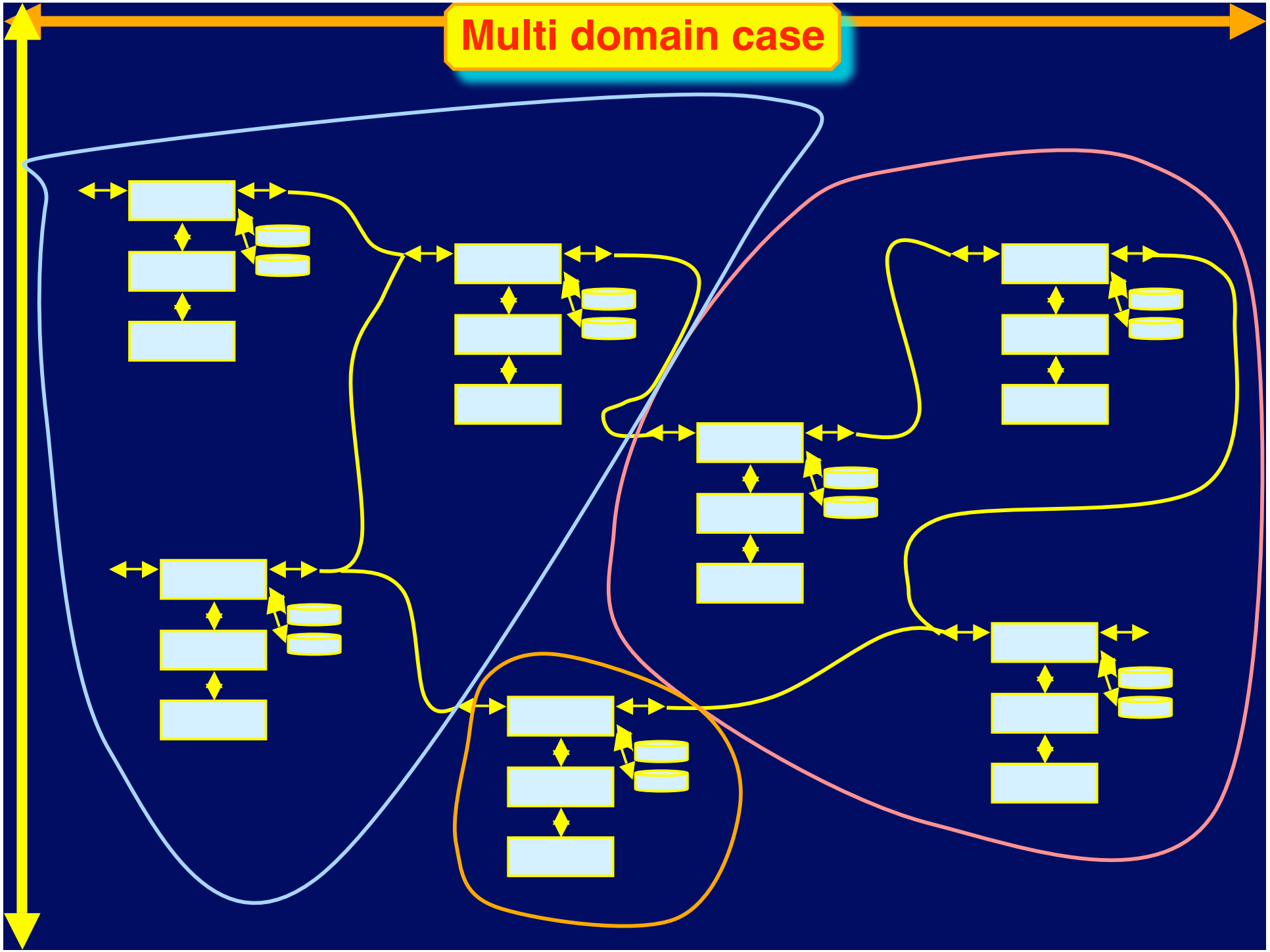

Authorization Models
AGENT
PULL
PUSH
USER
UHO
AAA
Service
Provider
1
2
3
4
5


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

The need for AAA



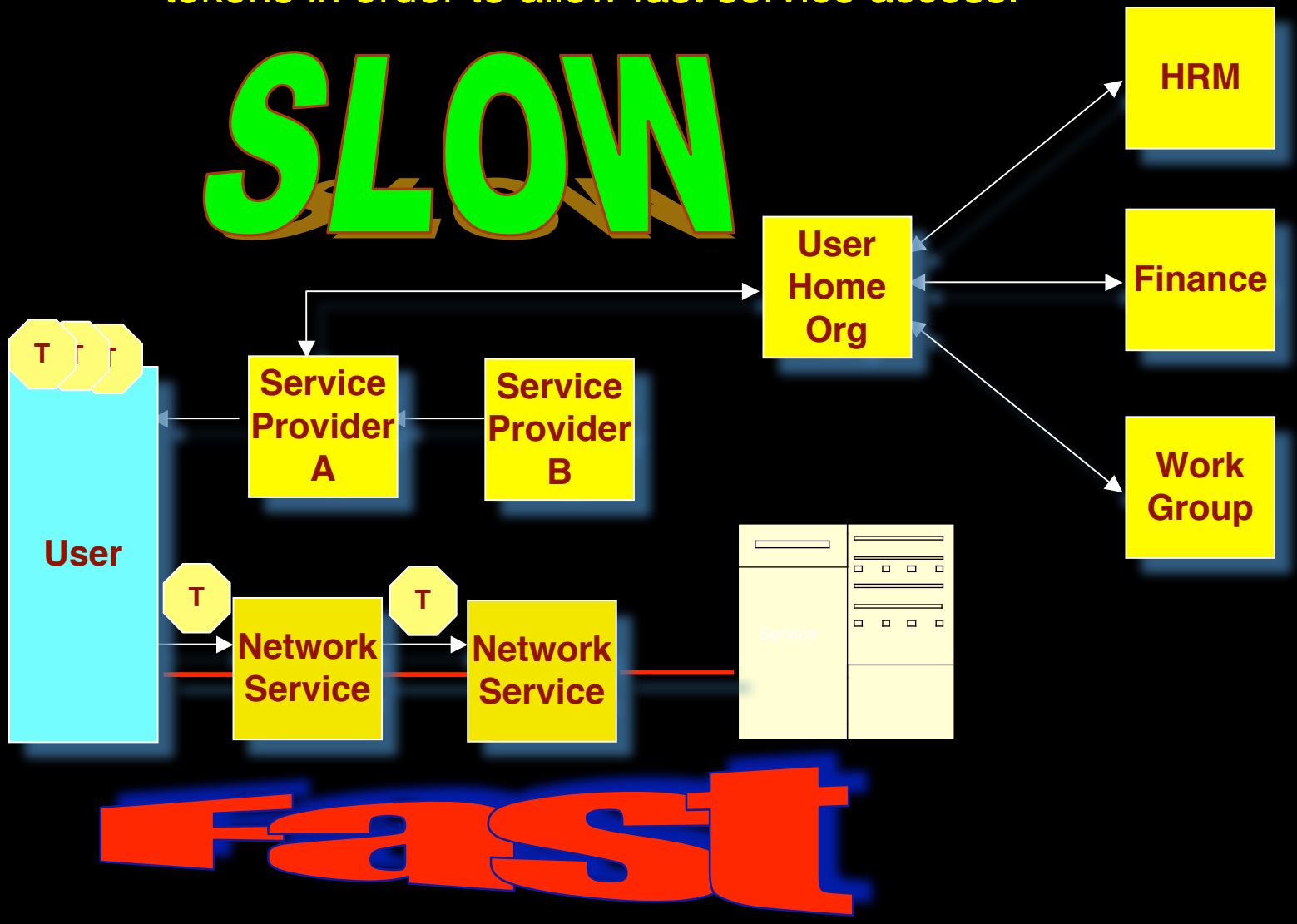

Roles
USER
USER
USER
UNI
UNI
UNI
SURFnet
DFN
SWITCH
REDIRIS
GEANT/DANTE


Multi domain case

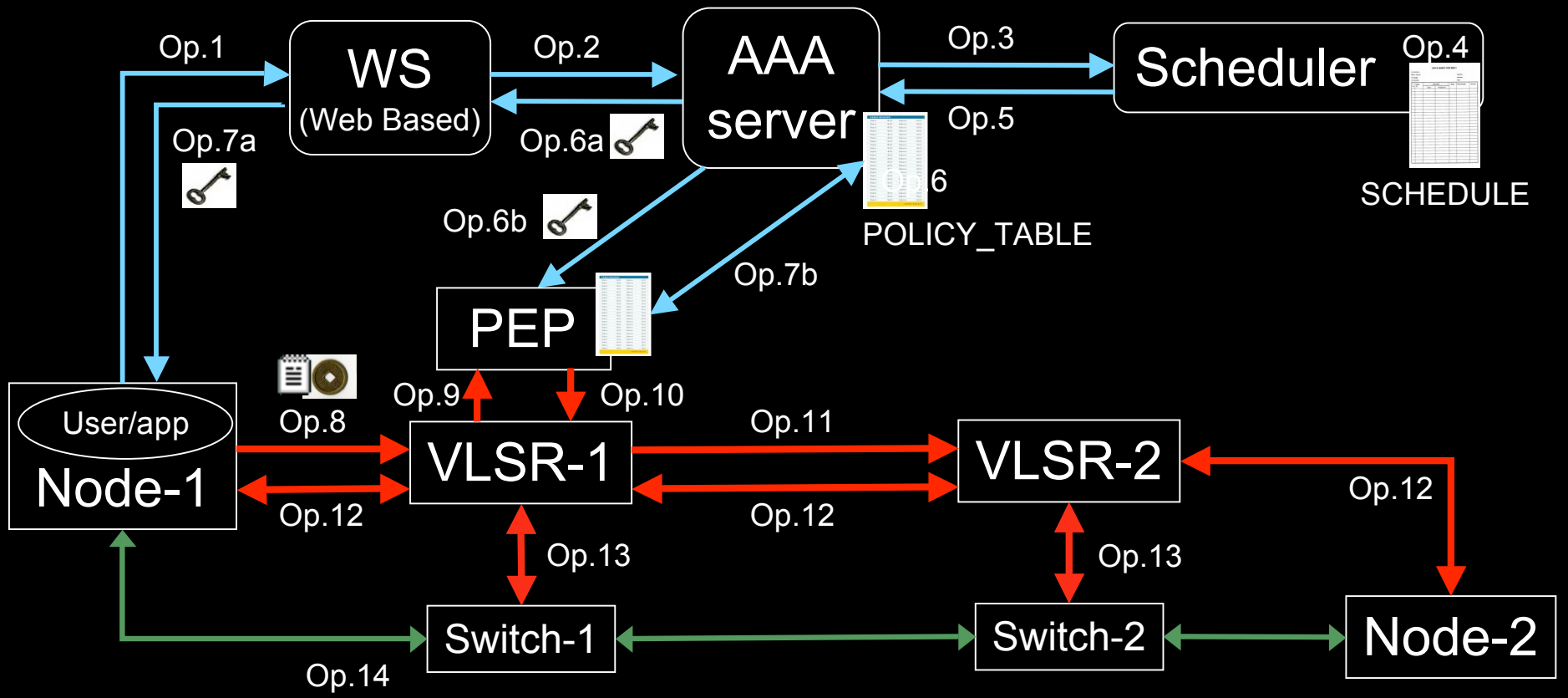
Simple service access

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.



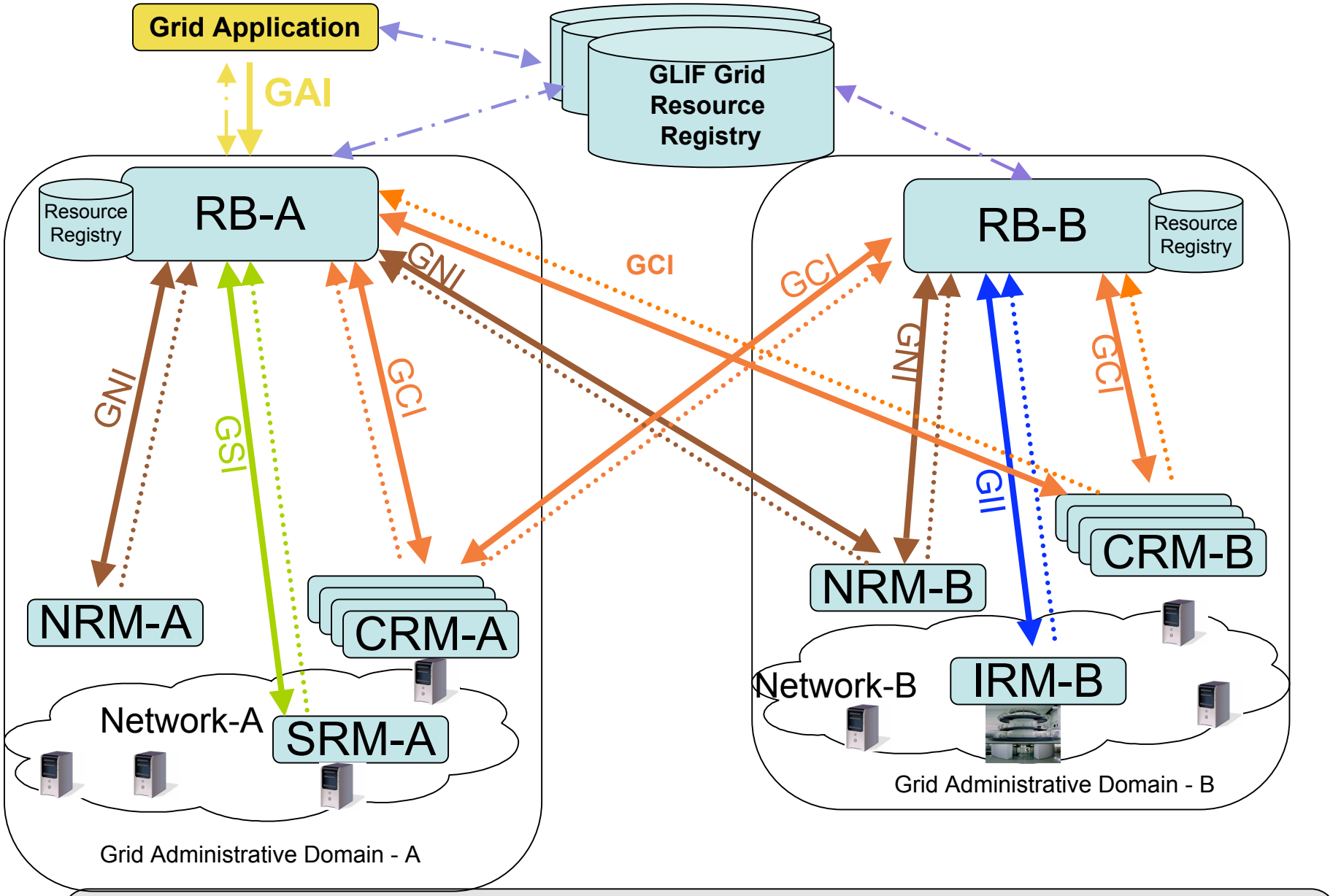
DRAGON GMPLS & TBN Demo, SC06 Tampa



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.

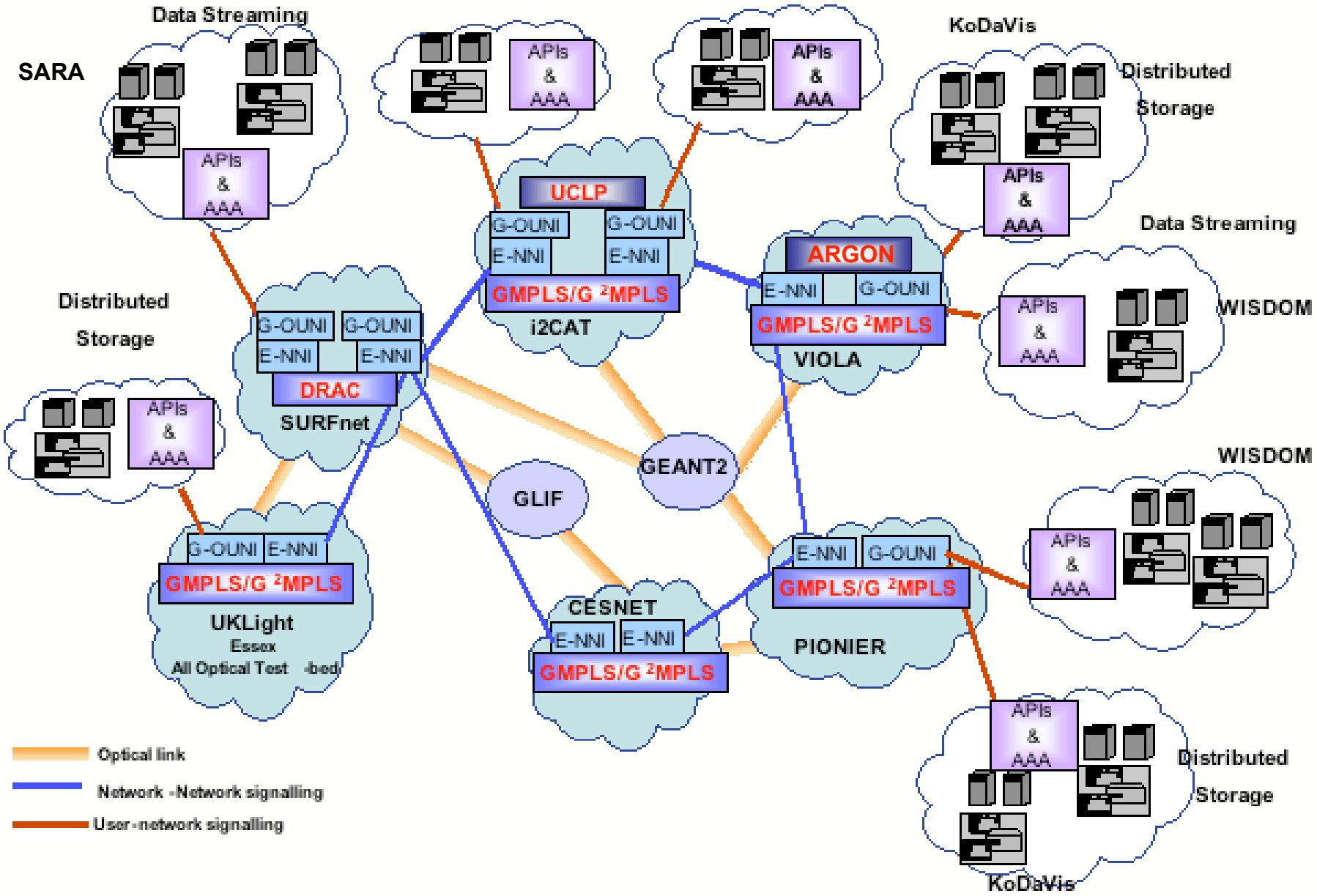
6a. AAA server issues an encrypted key to the WS.
6b. AAA server passes the same key to the PEP.
7a. WS passes the key to the user.
7b. AAA server interacts with PEP to update the local POLICY_TABLE on the PEP.

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
GAI
GLIF Grid Resource Registry
RB-A
Resource Registry
RB-B
Resource Registry
GNI
GCI
GSI
GII
NRM-A
CRM-A
SRM-A
Network-A
Grid Administrative Domain - A
NRM-B
CRM-B
IRM-B
Network-B
Grid Administrative Domain - B
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



Questions ?

AAARCH