

# *EuroCAMP and the European AAA and roaming activities*

APAN 2006, Tokyo

[Klaas.Wierenga@surfnet.nl](mailto:Klaas.Wierenga@surfnet.nl)

# Contents

- EuroCAMP
- Géant2 JRA5
- Federations for education
- Network access: *eduroam*
- Application access: eduGAIN

# EuroCAMP

- European CAMPUS Architecture Middleware Planning
- TERENA activity aimed at campus ICT-managers to fill the hole between
  - Innovators / NRENs and
  - Campus Managers
- Building on experience from Internet2

# EuroCAMP 2005

- 2 3-day workshops held in March in Turin (Italy) and in November in Porto (Portugal)
- Topics:
  - Identity Management
  - Federations for application (web) access
  - Federations for network access
- Expert speakers from Australia, USA and Europe
- Max. 100 attendees from universities all over Europe (and some abroad)
- Very well rated by the attendees
- The next EuroCAMP (March 2006, Slovenia) will focus on interoperability of federation software

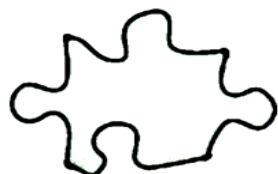


# Géant2 JRA5

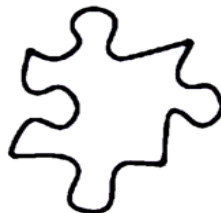
# Géant2 JRA5

- GÉANT2 is the pan-European research and education network, successor to the multi-gigabit network GÉANT.
- Connecting 34 countries using multiple 10 Gbps wavelengths
- GÉANT2 includes a programme of research and development initiatives, the Joint Research Activities (JRA's)
- JRA5 is on roaming and authentication/authorisation
- 16 NRENs participate in JRA5

# The JRA5 problem space



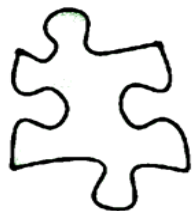
Network



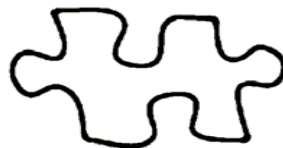
Authorisation



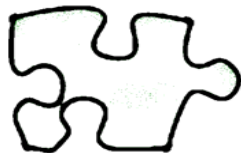
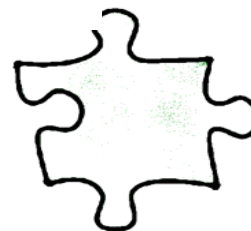
(web)Application



Authentication



Login



Administration



# JRA5

- JRA5 aims at building a pan-European infrastructure for AAA and roaming
- JRA5 consists of 2 major activities:
  - Building an authentication and authorisation infrastructure (AAI)
  - Building a roaming infrastructure based on *eduroam*
- In a separate single sign-on activity AAI and roaming will be combined
- The keyword is “federation”



Buzzword of the day:

# Federations

# Federations for education

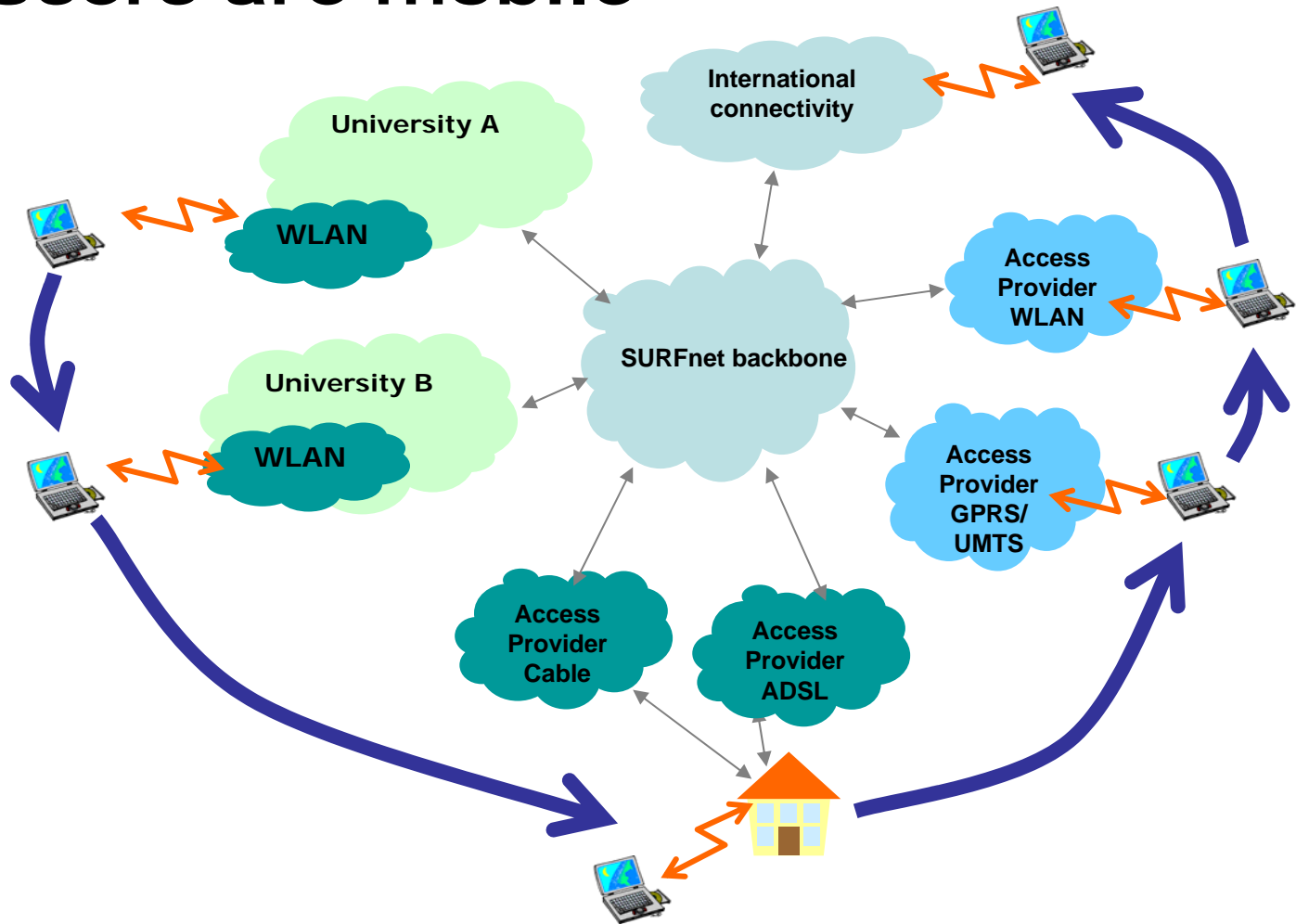
- Enable the sharing of educational resources
  - Network
  - Applications
    - Online learning systems
- Require agreement on:
  - Responsibilities
  - Liability
  - Technology
  - Language



Federation for network access

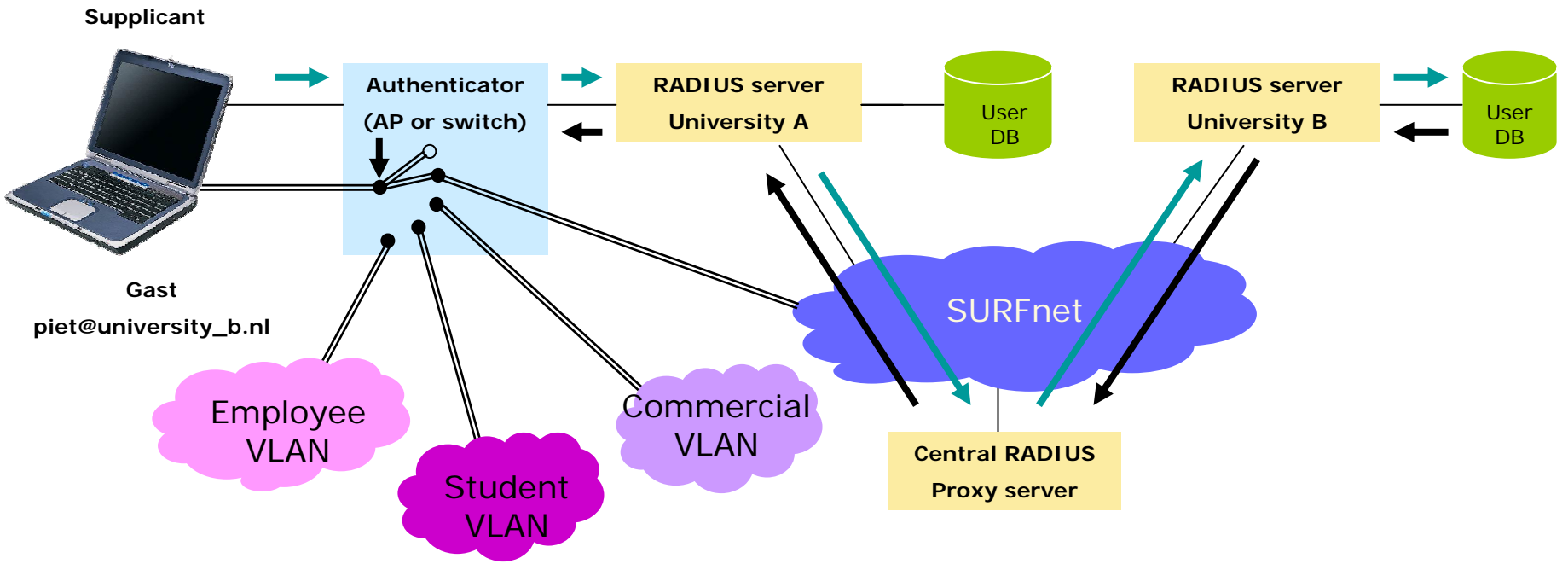
*eduroam*

# Users are mobile





# eduroam



Gast  
piet@university\_b.nl

→ signalling  
== data

- Trust based on RADIUS plus policy documents
- 802.1X
- (VLAN assignment)

# Status of *eduroam*



- Over 400 institutions in Europe, Australia and Taiwan
- USA, Sweden, Belgium will follow shortly

# Limitations of the current roaming infrastructure

- **Technology**
  - All authN and authZ traffic flows through the complete hierarchy
  - Static trust (shared secrets in preconfigured p2p chain)
  - Single points of failure
- **Policy**
  - Not suitable for full service yet, but test phase planned
- **Usability**
  - eduroam is not flexible enough with SSIDs, ciphers and VLANs mapping
  - Do we need a specialised client?
  - Where are the access points? Can a data base be helpful here?
- **Management & Monitoring**
  - Are all servers up and running?
  - How to detect abuse of the service?



# Federations for application access

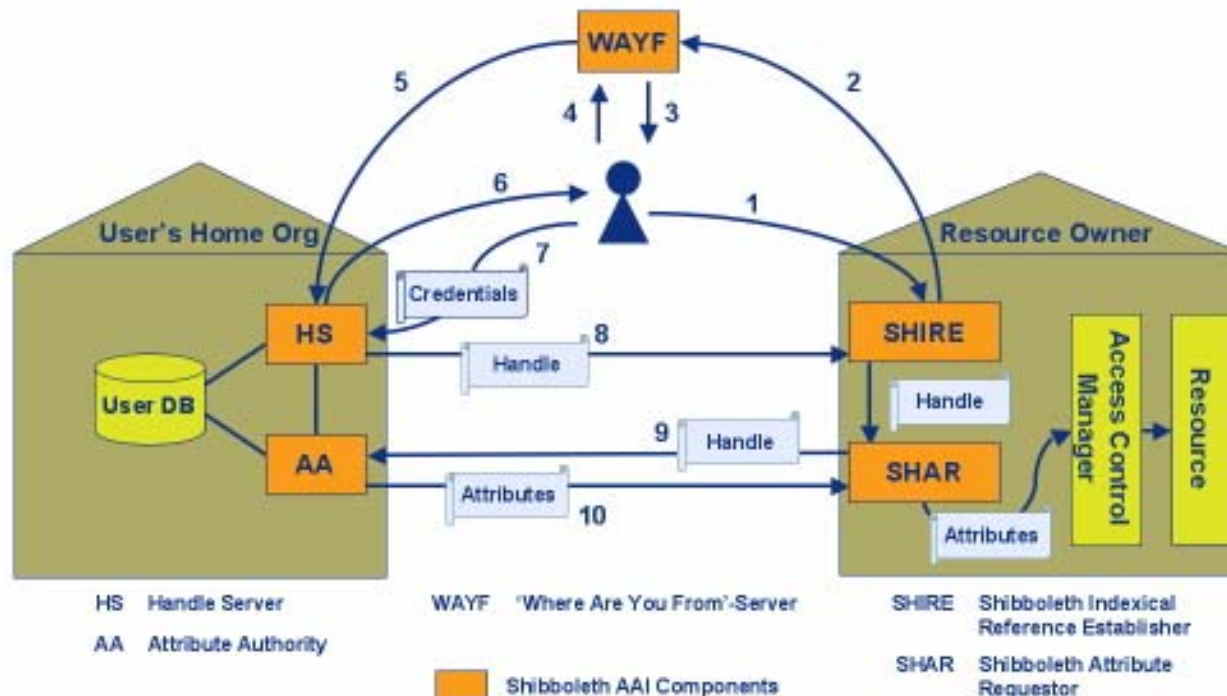
# eduGAIN



## Federation software in use in Europe

- A-Select
  - PAPI
  - FEIDE/Moria
  - CAS
  - PERMIS
  - SPOCP
  
  - and... Shibboleth
- How can we fit this together?

# Shibboleth

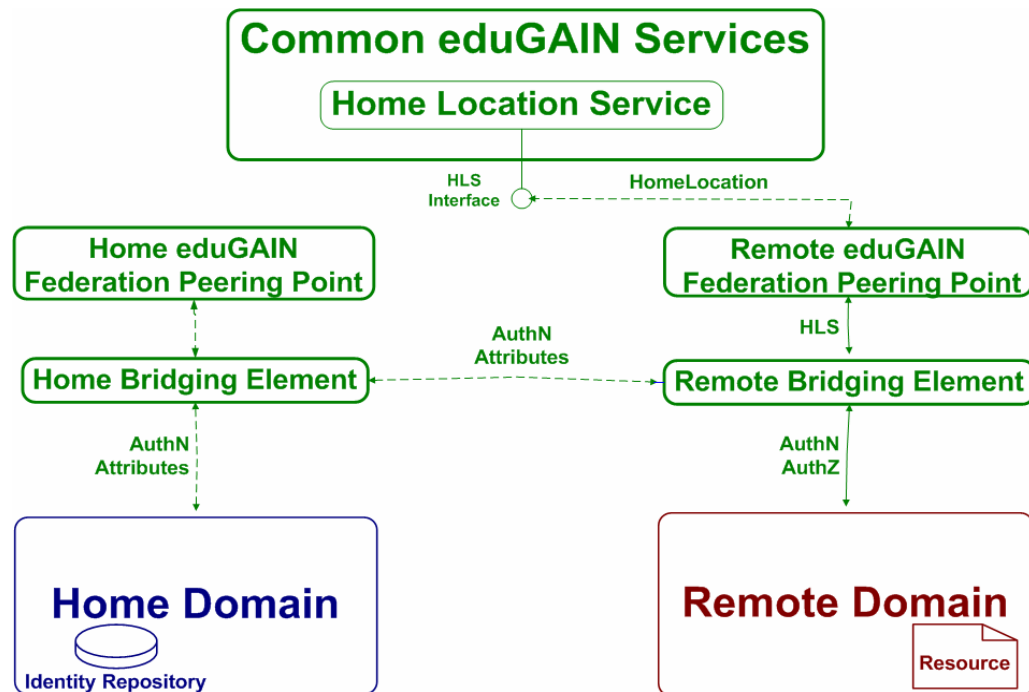


© SWITCH

- Allows institutions that belong to the same federation to share resources
- Lingua Franca: **SAML** (Security Assertion Markup Language)

# eduGAIN

- Goal: to federate federations
- **Web-services and SAML based**
- As much as possible Shibboleth compatible
- 4 basic interactions:
  - AuthnReq/Resp
  - HLSReq/Resp
  - AttrReq/Resp
  - AuthZReq/Resp
- Defining parameters, protocols and profiles



Existing solutions (Shibboleth, PAPI, A-Select etc.) will move to eduGAIN



# Conclusions



# Conclusions

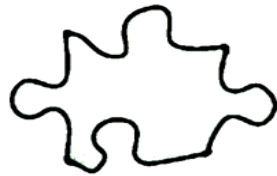
- To err is human, to federate is divine!
- Federation for network access: eduroam
- Federation for application access: eduGAIN

join.....

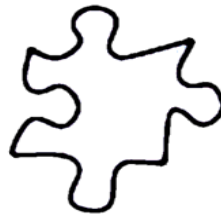


**eduroam**

# Turn the puzzle...



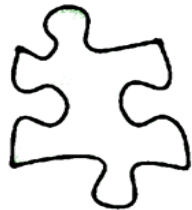
Network



Authorisation



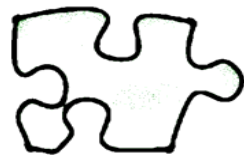
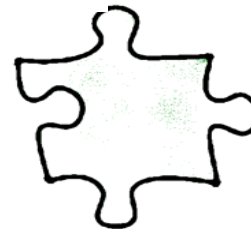
(web)Application



Authentication



Login



Administration



# Intro.....





# More information

- EuroCAMP
  - <http://www.terena.nl/tech/eurocamp>
- eduroam in SURFnet
  - <http://www.eduroam.nl>
- eduroam in Europe
  - <http://www.eduroam.org>
- TERENA TF-Mobility
  - <http://www.terena.nl/mobility>
- Géant2 Joint Research Activity 5 (authorisation and roaming)
  - <http://www.geant2.net/> (click on research)