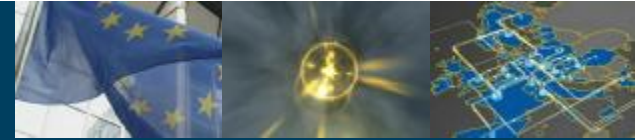


GN2 JRA5: eduroam transition to service

TtS meeting, 3rd technical workshop in Cambridge
J. Rauschenbach, DFN

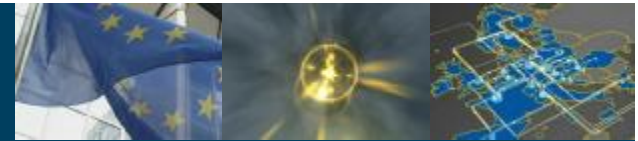


Connect. Communicate. Collaborate

JRA5 eduroam service

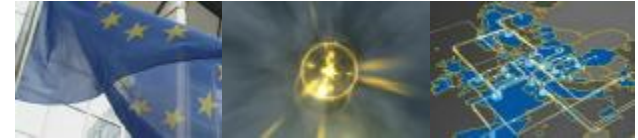
- The first JRA5 service will be the **eduroam confederation service**
 - Users will be the NREN based eduroam federations, providing the service to end users in their member institutions
 - The service will be conducted by the eduroamSA, that will establish the eduroam operational team (3-4 persons) for daily service handling.
 - According to our roadmap the service will start in April 2007
- eduGAIN is under development, no real testbed or pilot established by now, no production service possible in year 3 (some of the eduroam service procedures could be reused later on for eduGAIN)

Eduroam service description



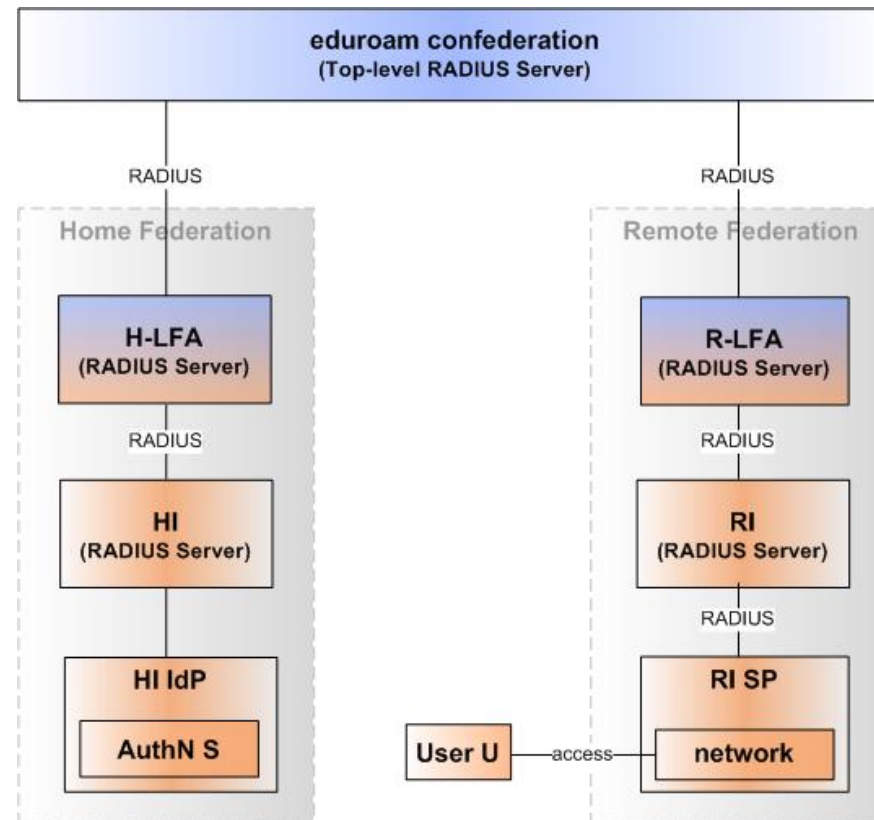
Connect. Communicate. Collaborate

- Roaming federation: network access at any location and at any time in the federation, providing nearly equivalent conditions as in the home institution (national or NREN level).
- Members of the federation are the institutions of the NREN constituency participating in the service.
- European eduroam confederation extends this service to all confederation members by
 - providing the necessary infrastructure to allow authentication at the home institution and by
 - defining the policy rules to ensure the necessary trust level.
- The service discussed here relates to the confederation!



eduroam confederation

Connect. Communicate. Collaborate



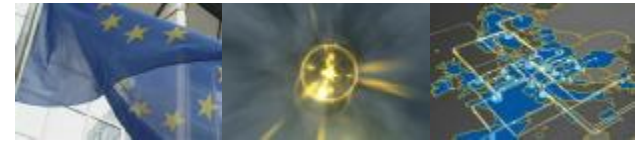
Operational model and user support



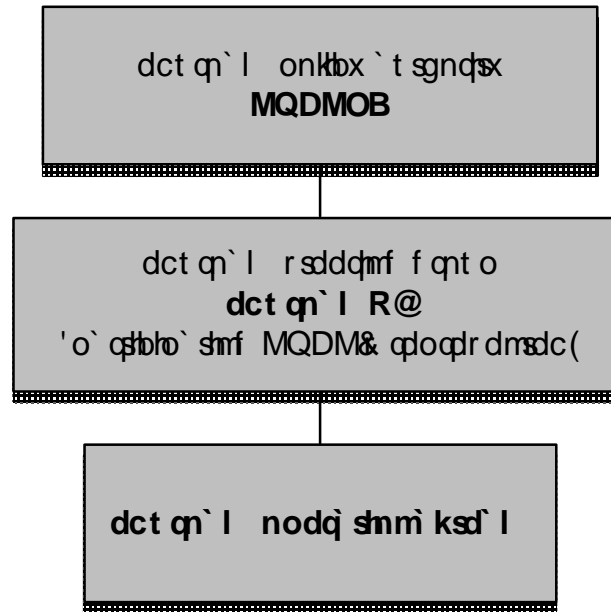
Connect. Communicate. Collaborate

- The overall eduroam infrastructure includes the following levels (multi-domain):
 - End user connects to a WLAN segment
 - Faculty/department level
 - Institutional level
 - Federation level (cctld or international organisation)
 - confederation level (EU)
 - multiconfederation (global) level
- Federations can be seen as users of the confederation service (and as roaming service providers for their members)
- End user support is assigned to the federation participant (institution), but the federation and the confederation operator can assist

eduroam organisational structure



Connect. Communicate. Collaborate

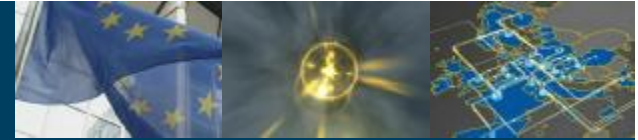




Connect. Communicate. Collaborate

Roles and Responsibilities

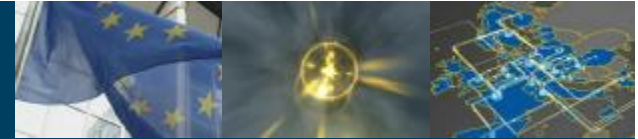
- **NREN PC:** eduroam policy authority
- **eduroamSA:** steer and guide the service
 - Formally eduroamSA could be installed as work item in SA3 or as service activity on its own - tbd
- **Operational team:** daily business, appointed by eduroamSA (needs EXEC approval to ensure funding)



Connect. Communicate. Collaborate

Policy agreement

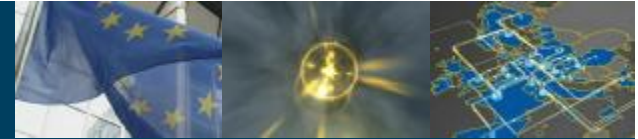
- Basic rules formulated in the policy document
 - Formal rules (how to join, to leave, liability)
 - Duties and rights of the participants, security requirements
 - Guidelines for a national federation policy included
 - Importance of the quality of the local Identity Management
 - Technical requirements and conditions, protocols
 - Web pages and AUPs, SSID
 - Web redirect transition period: October 06 - September 07
- The idea is to use the signed policy as a kind of service contract



Connect. Communicate. Collaborate

Related JRA5 Documents

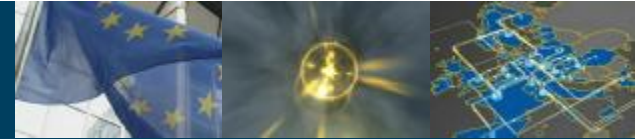
- JRA5 Glossary of Terms (DJ5.1.1)
- GÉANT2 roaming policy and legal framework (DJ5.1.3,1)
- Roaming requirements (DJ5.1.2)
- eduroam confederation policy document (DJ5.1.3,2)
- Description of the eduroam architecture (DJ5.1.4)
 - Evaluation of architecture alternatives
 - Background for the decision to bring RadSec on a standards track by writing an Internet-Draft for the IETF radext working group
- 1st version of the user guidelines document “Roaming cookbook”
DJ5.1.5,1 - installation help and configuration samples
- Plan for Transition of JRA5 Roaming into Production Service, DJ5.0.1



Connect. Communicate. Collaborate

Service availability

- DJ5.0.1 sets initial SLA (will be refined later)
 - Availability of the infrastructure in the range of 99%
 - Continuous monitoring (24/7), but helpdesk in normal working hours only
 - Definition of remedy procedures in case of a failure
 - Trouble Ticket System
 - Provisioning of contact details
 - Service reports
- Test facilities (end-to-end) additional to the monitoring platform needed, test accounts

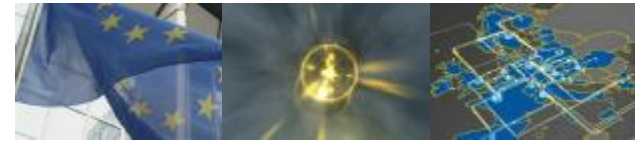


Connect. Communicate. Collaborate

Service providers

- Participants of eduroam can be found at www.eduroam.org
- Clickable maps provide more specific information on the federation level (not harmonised, but very useful)
- eduroam coverage data base would be helpful too

European eduroam participants

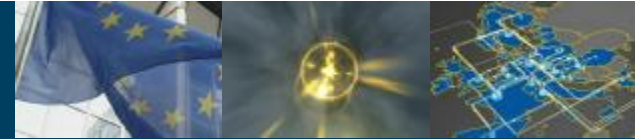


Connect. Communicate. Collaborate



JRA5 Team



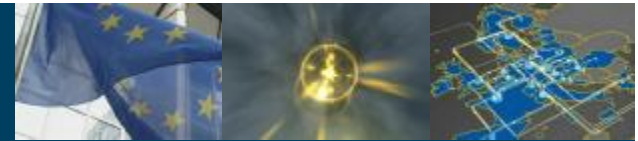


Connect. Communicate. Collaborate

eduroamSA

- Starting point: current European eduroam pilot plus policy agreement (to be signed by confederation participants), was provided in November 2006
- eduroam service activity (eduroamSA) principles:
 - Follows the Access Point Manager (APM) model
 - Representatives from European eduroam participants (29 NRENs or liaised local operators, TERENA, Dante)
 - Not every operator **MUST** be in the eduroamSA from the start (though recommended)
 - The eduroamSA will be open to invite experts not acting as local operators, but bringing in expert knowledge
 - eduroamSA is different from JRA5 and from TF Mobility, but exists in parallel (some overlap is very likely to happen), non-JRA5ers are not only welcome, but needed!

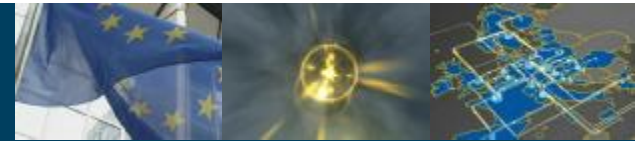
eduroamSA tasks



Connect. Communicate. Collaborate

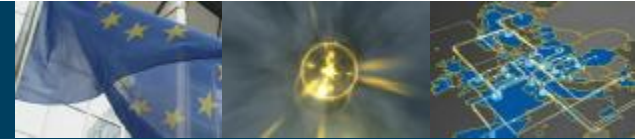
- Main task of eduroamSA is to steer the work on the eduroam service:
 - Recommendations on diagnose tools and scripts to be used
 - Further policy development in coordination with JRA5/TF M
 - Integration of further results from JRA5/TF Mobility
 - Application of trust means (eduGAIN CA)
 - Dissemination work (maintenance of the web pages, enhancement of the visibility of eduroam including the provision of promotional material)
 - Collection of usage related data and publication of graphs and statistics
 - Support for new members (material collection, contact point)
 - Organisation of training events or programs (together with NA8, eduroamSA and JRA5 for content)
 - Virtual home of the operational team

Eduroam operational team tasks



Connect. Communicate. Collaborate

- Operational team is doing the daily work:
 - Running the confederation infrastructure incl. top level servers and associated services
 - Monitoring the confederation and federation level servers
 - Development/adaptation of diagnose tools and supporting scripts
 - Handle fault resolution procedures
 - Technical support for new members, provisioning of test facilities
 - Coordination of trust means (eduGAIN CA, CRLs)
 - Gathering of statistics on eduroam usage, error reports



Connect. Communicate. Collaborate

Roadmap (proposal)

- The roadmap proposal is part of DJ5.0.1:
 - date of policy approval by the NREN PC was August 06
 - derivation and distribution of a stand-alone policy agreement in November 06
 - formal establishment of the eduroamSA in January 2007 (3rd TWS)
 - appointment of the eduroam operational team at the first meeting of eduroamSA in January 07
 - collection of signed documents during a sufficiently long transition time until February 07
 - technical add-on's (monitoring, RadSec, ...) until March 2007
 - official service start April 2007

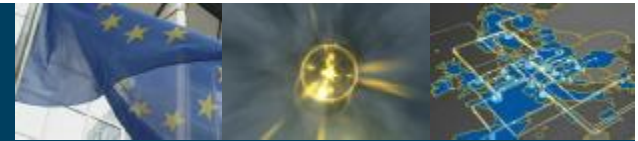


Connect. Communicate. Collaborate

Risk analysis

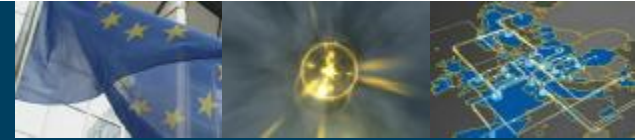
- National legal regulations might be difficult to handle
 - Anti-Terror laws
 - Closed user group issue
- Number of participants is crucial
 - In the confederation participating federations
 - The coverage of institutions participating in the federations!
- Availability of the components of the confederation infrastructure has an impact on the stability and performance of the service

Additional support for roaming federations



Connect. Communicate. Collaborate

- Well developed federations with a good coverage are essential for the success of the confederation service. The following items can be supported to enforce the rollout:
 - collect and provide local information in a concerted manner
 - English web pages (if not yet available)
 - financial support for SW/HW (e.g. Radiator, a number of AP for test or support for newcomers)
- The idea is to provide a small funding to those being in the rollout and those willing to help

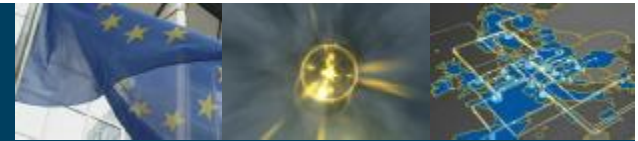


Connect. Communicate. Collaborate

Funding of eduroamSA

- The following roles shall be funded with approx 0,5 FTE:
 - eduroamSA leader (work item leader in SA3 or new SA)
 - Operational team member (3-4 persons working with eduroamSA participants, recommendation: when the organisation the eduroamSA leader comes from is in the operational team as well)
 - Funding scope: eduroamSA start (Jan 07) until project end
- The normal eduroamSA participants might apply for funding in the range of 1 – 2 person months in year 3 (including travel support to ensure 3 meetings per year), according to their needs or willingness to invest time and effort to help newcomers, rollout phase only
- Funding scope: eduroamSA start (Jan 07) until project end
- Participation and interest in a small funding should be reported to the eduroamSA leader urgently!

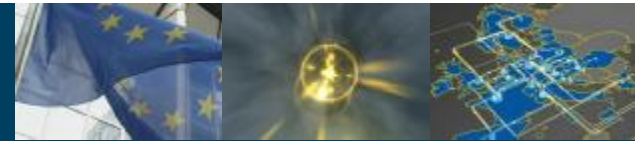
Questions



Connect. Communicate. Collaborate

?

eduroam architecture alternatives (DJ5.1.4)



Connect. Communicate. Collaborate

- **RadSec** (OSC, modification of the RADIUS protocol)
 - ü Uses TCP/SCTP instead of UDP
 - ü TLS tunnels used between servers: authentication is based on certificates instead on IP addresses, RADIUS packet transported in the tunnel (encrypted), no shared secrets needed
 - ü Experimental work done (and integration into pilot planned)
 - ü Dynamic peer discovery in beta state
 - Not a standard solution (yet), not all RADIUS implementations for now, but good signals from FreeRadius
- **DIAMETER** (RFC 3588)
 - Problem: no DIAMETER “quality” implementation so far
 - ü DAME will use openDIAMETER and provide transfer agents
- **RADIUS/DNSSec**
 - Look-up through secure DNS (not very much in use)
 - Dedicated roaming domain secure DNS tree needed