

National and International Joint Research Activities: The JRA5 view

3rd Concertation meeting on e-Infrastructure,
Helsinki

20 November 2006

Jürgen Rauschenbach, DFN-Verein, jrau@dfn.de



Connect. Communicate. Collaborate

Problem and JRA5 vision

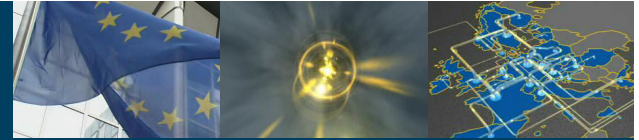
- How to organise access to resources in the research and education area (networks, digital documents, computer power etc) in a sufficiently safe and easy to handle way?
- JRA5 Vision:
 - 1) To build a roaming infrastructure enabling full mobility of members of the scientific community in Europe across institutional campuses. **“open your laptop and be online”**
 - 2) To build an interoperable authentication and authorisation infrastructure that will be used all over Europe enabling seamless sharing of e-science resources.
 - 3) To develop and pilot a single sign-on system enabling a *log in once* experience for network and application access, even beyond organisational boundaries.



Connect. Communicate. Collaborate

Federations – why?

- Synergy effects, joining a federation instead of many bilateral agreements, purpose based (one for all?)
- Different communities, different needs
 - Not even talking about international collaboration
 - Different technical and organisational solutions
 - Digital libraries, e-learning, Grids as current examples
 - More to come: Governments, professional associations, commercial operators,...
- Don't hold your breath waiting for the Real And Only Global Federation



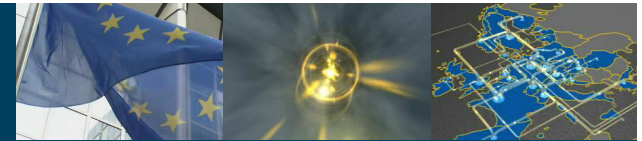
Connect. Communicate. Collaborate

Federation ingredients

- Identity management is key!
- Agreeing on trust mechanisms (PK technologies, component IDs)
- Aligning on schemas (eduPerson, SCHAC, ...)
- Reaching applications
- Coordinating metadata
- SAML for identity data exchange (moving to SAML2)
- Policy

- JRA5 currently focuses on the following AA systems : Shibboleth, Liberty Alliance, PAPI, A-Select

Confederations: Federate Federations



Connect. Communicate. Collaborate

- Same federating principles applied to federations themselves
 - Own policies and technologies applied locally
- Independent management
 - Identity management, authentication/authorization must be properly handled by the participating federations and federation participants
- Confederation policy
 - Linking individual federation policies
 - Coarser than the linked federation policies
- Trust fabric entangling participants
 - Through each federation's fabric
 - P2P trust must be built dynamically



Connect. Communicate. Collaborate

JRA5 current work

- eduroam.:
 - Preparation of the eduroam service (organisational)
 - Technical enhancement of the current infrastructure
- eduGAIN:
 - Implementation of the components of the AAI architecture according to the specification and creation of test cases
 - Development of a profile for the specific requirements of GN2 activities (JRA1 based right now)
- SSO:
 - Definition of SSO requirements and provision of SSO concepts that match these requirements

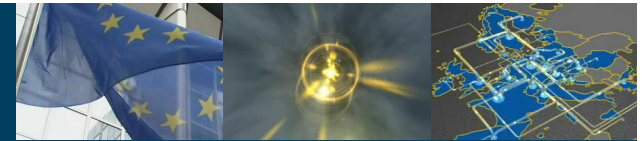


JRA5 Transition to Service

Connect. Communicate. Collaborate

- First JRA5 service: European **eduroam confederation service** (eduGAIN is planned to follow later on)
- Roadmap: service will start in April 2007; the eduroam confederation policy document is ready for signing by the NRENs
- “Users” will be the NREN based eduroam federations, providing the service to end users associated with 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.

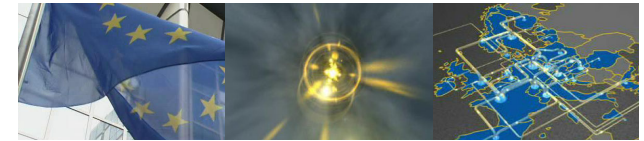
European eduroam confederation principles



Connect. Communicate. Collaborate

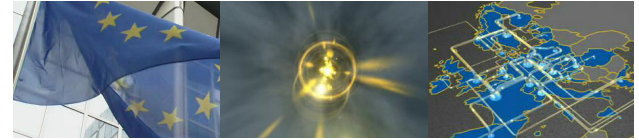
- Mutual access – no fees
- Authentication at home - Authorisation at visited institution
- Home institutions are/remain responsible for their users abroad
- Members are **European** NRENs
- Members guarantee required security levels by their participants
- Members promote eduroam in their countries
- European eduroam may peer with other regions (confederation level)

European eduroam participants



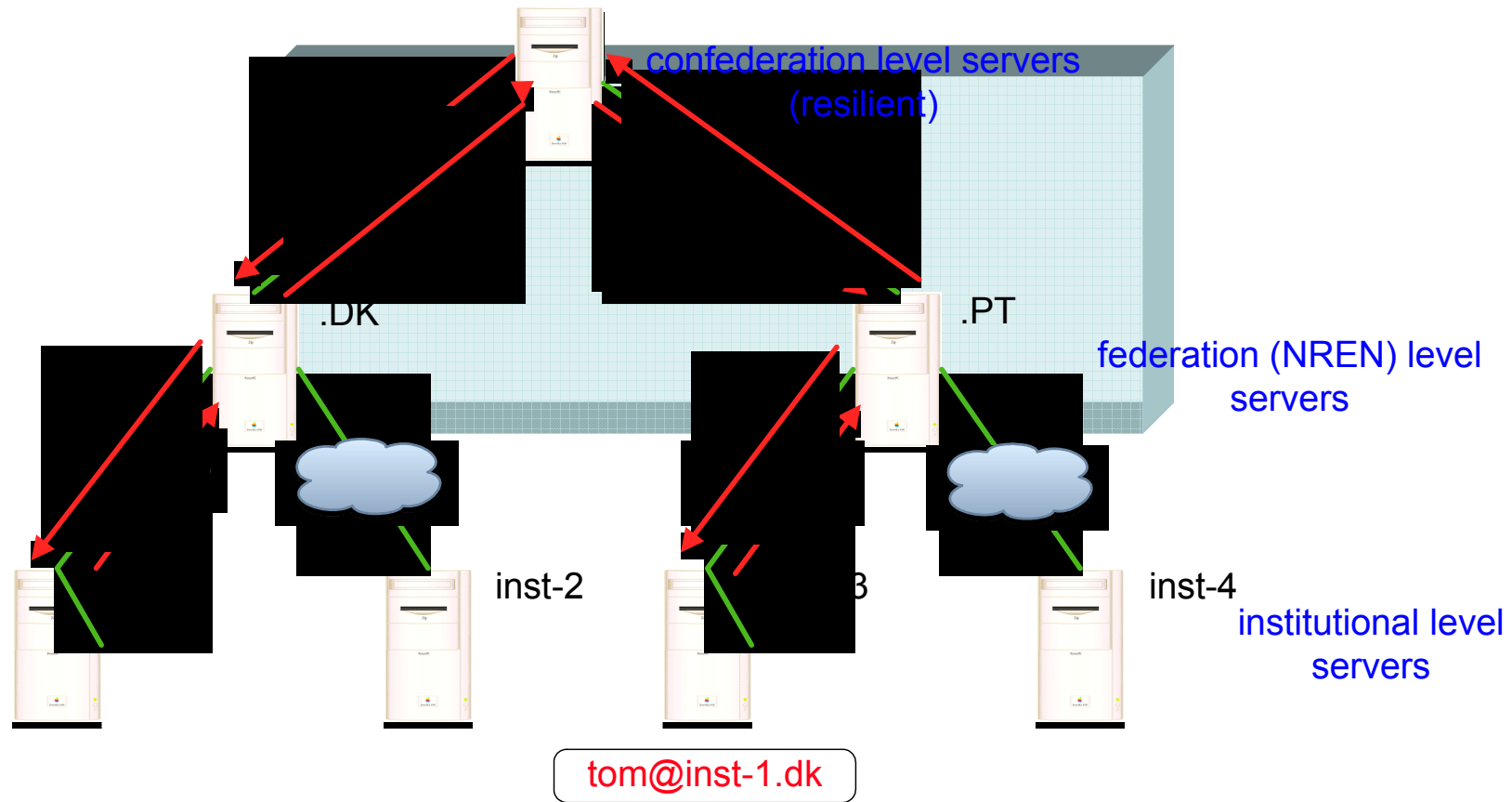
Connect. Communicate. Collaborate





Eduroam RADIUS hierarchy

Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

eduGAIN related work done

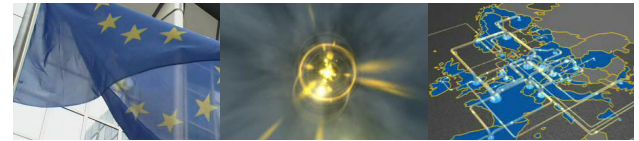
- AAI achievements – exercising the confederation concepts
 - Specification of the AAI architecture (DJ5.2.2) – new version end of November
 - Implementation of the AAI basic components
 - Start of implementation of bridging elements (Shibboleth, Liberty Alliance/FEIDE, PAPI)
 - Development of the initial 2 profiles (web services, automated clients)
 - Support of the GÉANT Identity Provider (GIaP) project
 - Guidelines for connecting to eduGAIN document “AAI cookbook” DJ5.2.3,1 available <http://www.geant2.net>



Connect. Communicate. Collaborate

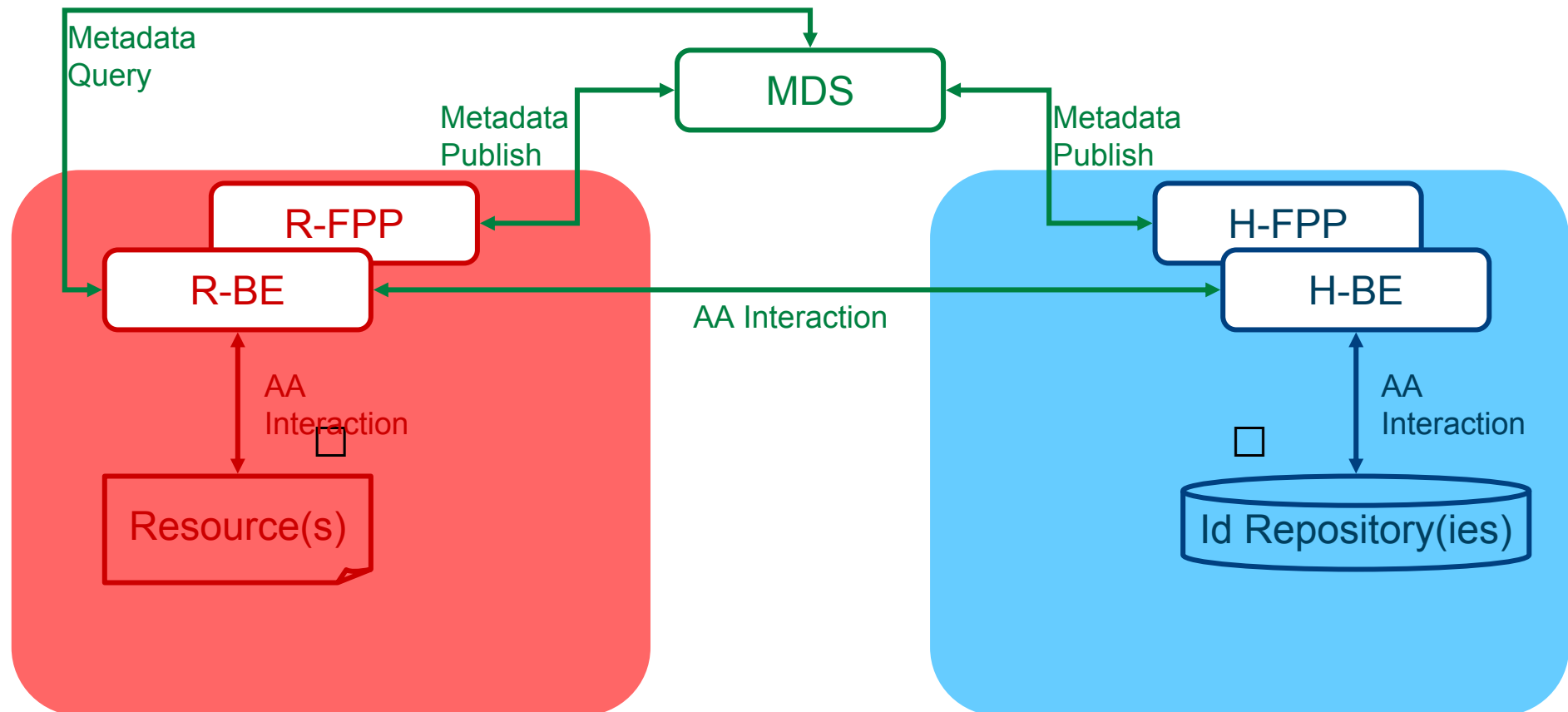
The eduGAIN Components

- Bridging Elements (BE)
 - Interconnection points
 - Federation-wide (LFA) or distributed (LA)
- Federation Peering Point (FPP)
 - Able to announce BE metadata
- The Metadata Service (MDS)
 - Centralised metadata storage, distributed publishing and trust
 - Publishing interface (for FPPs and authorised BEs)
 - Querying interface (for BEs)



Connect. Communicate. Collaborate

The eduGAIN Model





Connect. Communicate. Collaborate

Operation Mapping

- Maps the abstract service definition into actual protocols
- Current version is based on SAML 1.1
 - Profiling the standard to fit abstract parameters
- A SAML 2.0 implementation will be available along the lifetime of the project
 - The abstract service specification protects components and applications from these changes
- Authentication assertions and attribute exchange mechanisms are designed to be Shibboleth 1.3 compatible (and Shibboleth 2 in the future)



Connect. Communicate. Collaborate

Conclusions/Summary

- eduroam transition to service progressing
- Rollout needs support by participating NRENs
- AAI component implementation almost complete (eduGAIN)
- Initial profiles defined
- Tests with real federations soon
- Forming an eduGAIN confederation by adding a policy to the infrastructure is on our agenda
- SSO requirements and model under discussion