



GN2 JRA5 update

Jürgen Rauschenbach (DFN),

JRA5 team

04/02/08 Marseille



Connect. Communicate. Collaborate

eduroam

- Working on the eduroam database and a new dissemination look (maps)
- RadSec release 1.0 Beta is out - reasonable stable and some new features (server failover)
- IETF items under preparation
- Service specification is finished, policy part too, sent by Dante to the NRENs (more in TF Mobility by Miro)



eduGAIN characteristic

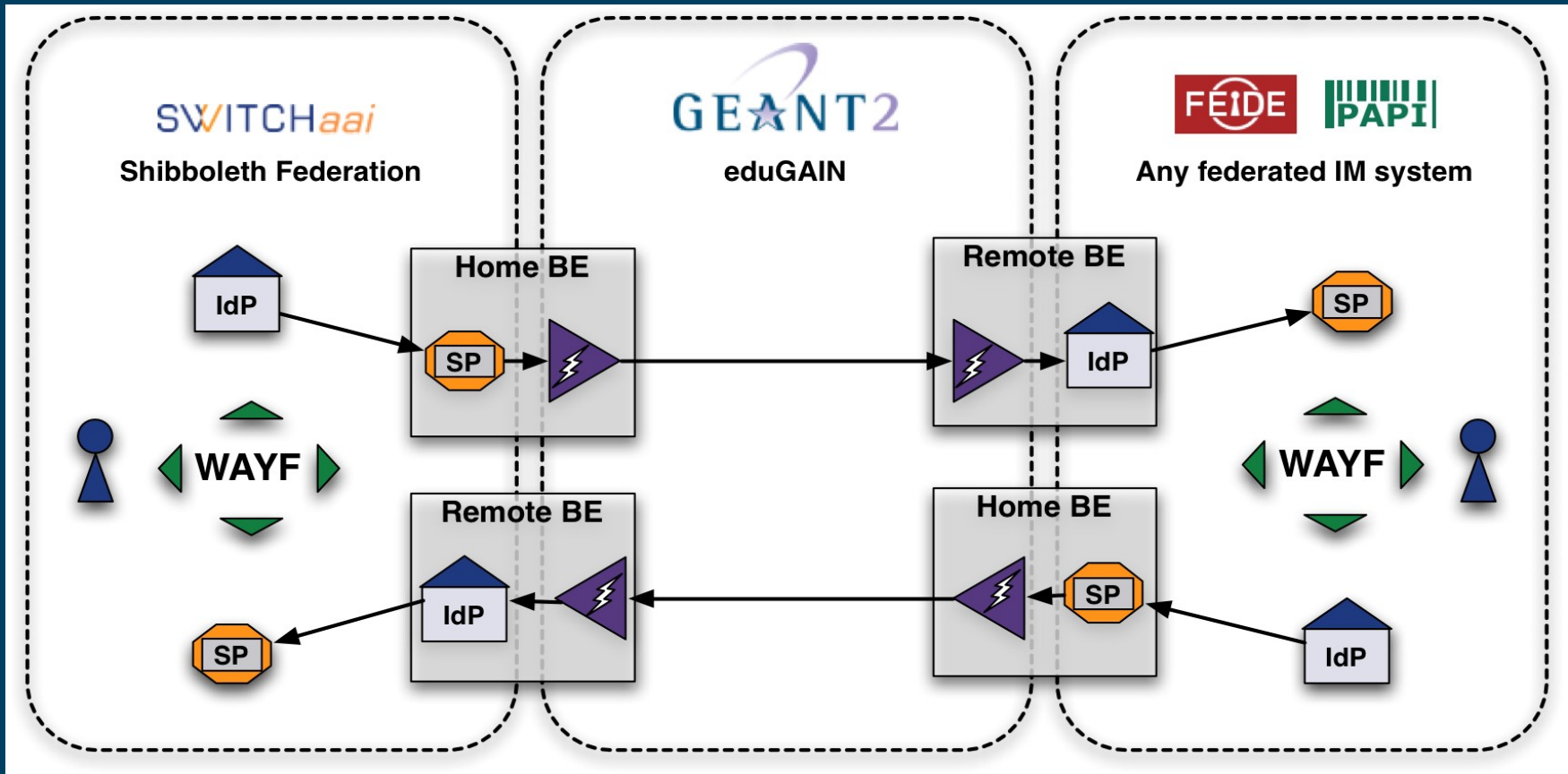
Connect. Communicate. Collaborate

- Based on the national federations, operated by NRENs
 - InCommon, SWITCHaai, HAKA, Ukerna/JISC, DFN-AAI, GRNET, HUNGARNET, ...: Shibboleth
 - Feide, RESTENA, UNI-C (DK), GIdP, ...: simpleSAMLphp
 - SURFfederatie: A-Select
 - RedIRIS: PAPI
 - Edu@HR: RADIUS-based
- eduGAIN is a confederation infrastructure (for all above mentioned AAI systems eduGAIN BEs exist)
- Different technologies, but
 - SAML1.1/SAML2.0 is Lingua Franca
 - eduGAIN and most other AAI systems provide interoperation with Shibboleth (directly or via especially developed gateways like eduGAIN BEs)



BE Infrastructure

Connect. Communicate. Collaborate



eduGAIN current work areas



Connect. Communicate. Collaborate

- Putting the pieces together
- Extending the testbed by other federation systems, new locations, and functionality
- First applications are operational (JRA5 wiki, CoManage, perfSONAR and AuthBAHN profiles),
- More applications are planned: federated tools to be used by project participants (how to protect applications not being built this way?)
- Start thinking about an eduGAIN service (policy again!)

Where are we with eduGAIN?



Connect. Communicate. Collaborate

- Stabilising eduGAIN components and interoperation in an eduGAIN pilot
 - Deployment of BEs
 - Stable software distribution, urn registry and PKI (web pages are operational for test), eduGAIN test means
 - Integration with GIdP (SA3)
 - Integration and operational usage with perfSONAR (JRA1)
 - Integration and operational usage with BoD (AutoBAHN, JRA3)
 - More ideas around (OTRS for SA5, SA6, bug tracking ...)
- Further aspects:
 - integrate roaming with the European AAI eduGAIN (DAME)
 - Expanding the set of BE implementations and profiles

Confederation Service Elements



Connect. Communicate. Collaborate

- Metadata Service MDS
 - Repository of metadata of all connected IdP and SP
 - Upload by authorised components (FPP/BE)
 - Queries possible, WFAYF for user selection or automated
- PKI: component ID used in certificates, certification requests, CRL, CP/CPS
- URN: components names, protocols etc
- Web site: www.edugain.org portal and info
- Attribute mapping or Credential Conversion service (different schemas might be used)
- Elements still under development!

Infrastructure support elements (to develop)



Connect. Communicate. Collaborate

- Monitoring (AAIEye or other, not yet there)
- Trouble Ticketing System (probaly OTRS)
- CMDB, reporting, other ITIL features n.a. yet

- Operational Support Team and help desk
 - Central components operation and maintenance
 - Trouble shooting between different AAI systems
 - Support from development group
 - Training for federation operators



DAMe status

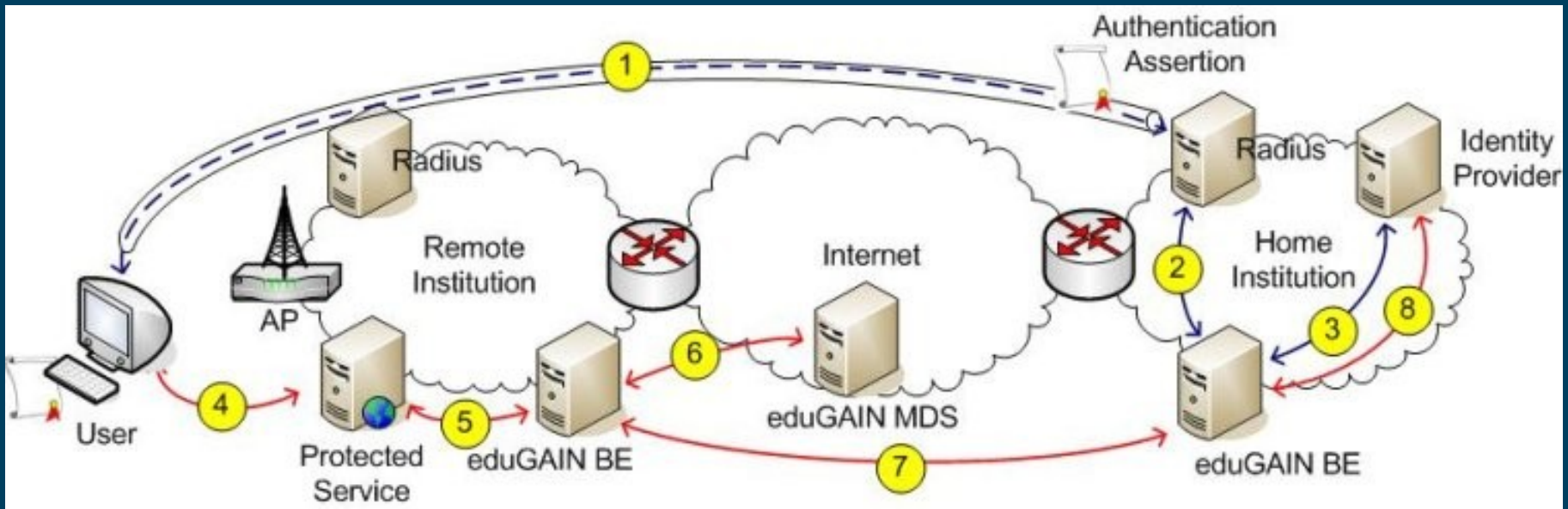
Connect. Communicate. Collaborate

- Report in TF Mobility (Sascha)
- Needed SW components developed, testbed installed
- BE-like solution available for Shib and PAPI
- uSSO architecture document will be out soon



DAMe proposal for uSSO

Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

Confederation Policy

- Do we need a written confederation policy? Sign it?
- Yes. Reasons:
 - To build the trust system (IdPs must be run according to some rules, LoA?)
 - High level decision: permission to upload metadata
 - Cooperation in case of problems
 - Attribute set and schema, mapping rules
 - Organisational requirements (web pages for confederation service should be supported by federations, federation have to provide web pages as well and publish their own policy, ...)