



GN2 JRA5: Roaming and Authorisation - recent results

Jürgen Rauschenbach (DFN),
Klaas Wierenga (SURFnet),
Diego Lopez (RedIRIS),



Connect. Communicate. Collaborate

Content

- Overview
- Roaming infrastructure
- AAI



Connect. Communicate. Collaborate

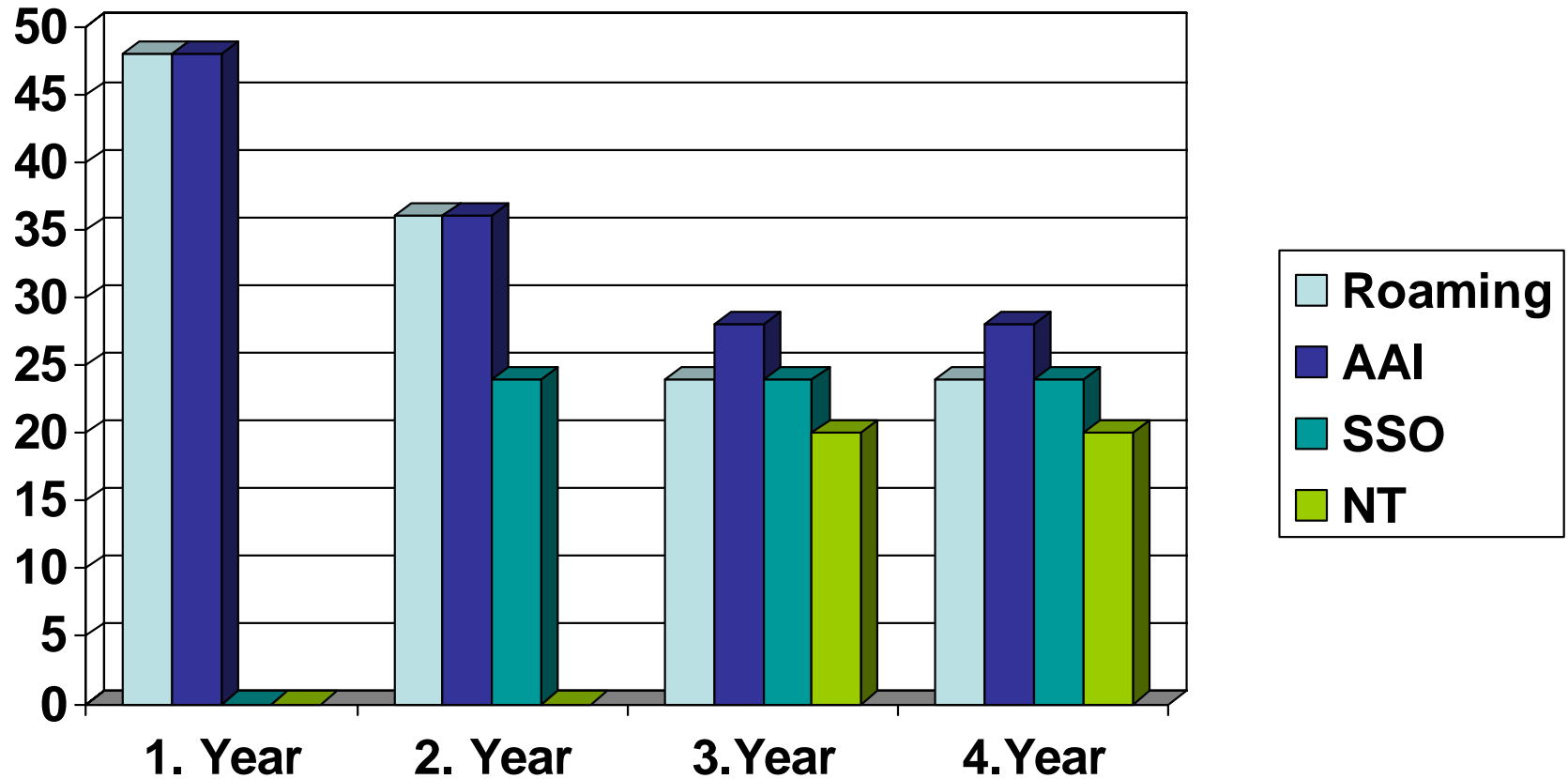
Structure and Partners

- JRA5 consists of the following Work Item in the 4 project years:
 - WI-1: Roaming
 - WI-2: Authentication and Authorisation Infrastructure
 - WI-3: Single Sign-On
 - WI-4: Integration of advanced Technologies
- 16 NRENs + Dante, 97 participants (mailing list) from 18 countries, with around 35 contributing persons
- Partners are SURFnet, DFN, RedIRIS, NORDUnet (University of Umea, UNI-C, UNINETT, CSC); ARNES, CARNET/SRCE, CESNET, FCCN, GRNET, HEAnet, HUNGARNET, ISTF, RESTENA, SWITCH, Ukerna, Dante
- Collaboration with many external groups: TF-Mobility, TF-EMC2, GN2 activities (JRA1, SA3), international groups like eduroam gwg, Internet2 (FWNA), Grids, ...



Work item distribution

Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

Achievements

- Work item 1 (Roaming) deliverables
 - “Glossary of Terms” **DJ5.1.1**, a terminology document
 - “Roaming Requirements document” **DJ5.1.2 (*)**; security, standardisation and operational requirements
 - “legislation overview” for roaming **DJ5.1.3-1** part 1
 - “confederation policy” is delayed, in draft state: **DJ5.1.3 part 2**
 - Roaming architecture is in draft state **DJ5.1.4 (on track)**



Achievements (2)

- Work item 1 technical focus points:
 - extension of the roaming pilot “eduroam”, both
 - in the number of participants (NRENs) and also
 - functionally (analysing the current infrastructure, eduroam-in-a-box, alternative and enhanced architecture discussion).
 - co-operational work with the TF Mobility, usage of the eduroam pilot as experimental platform in JRA5 as a step stone to eduroaming. Open discussion and dissemination on the mobility list.
- Work item 1 political focus points:
 - Legislation overview
 - Policy document: European confederation policy
 - Significant change in December 05 in the organisational structure
 - we hope to reach consensus soon



Connect. Communicate. Collaborate

Achievements (3)

- Work item 2 AAI deliverables
 - “AAI Requirements document” **DJ5.2.1** (February 05)
 - “AAI architecture document” **DJ5.2.2** (October 05)
- Work item 2 focus points
 - architecture design (structure and components, operations definition, formal specification, Internal implementation paper drafted)
 - Oriented on web services, but other application areas not excluded
- Coordination liaisons
 - Internal: Other activities as potential users of AAI
 - Specific profiles under discussion
 - External
 - EC e_Concertation activities
 - Internet2 (USA): MACE, EuroCAMPs, NorthAmerica-Europe coordination group
 - Upcoming: MAMS (Australia)



Connect. Communicate. Collaborate

Content

- Overview
- Roaming infrastructure
- AAI



JRA5 Team





eduroam

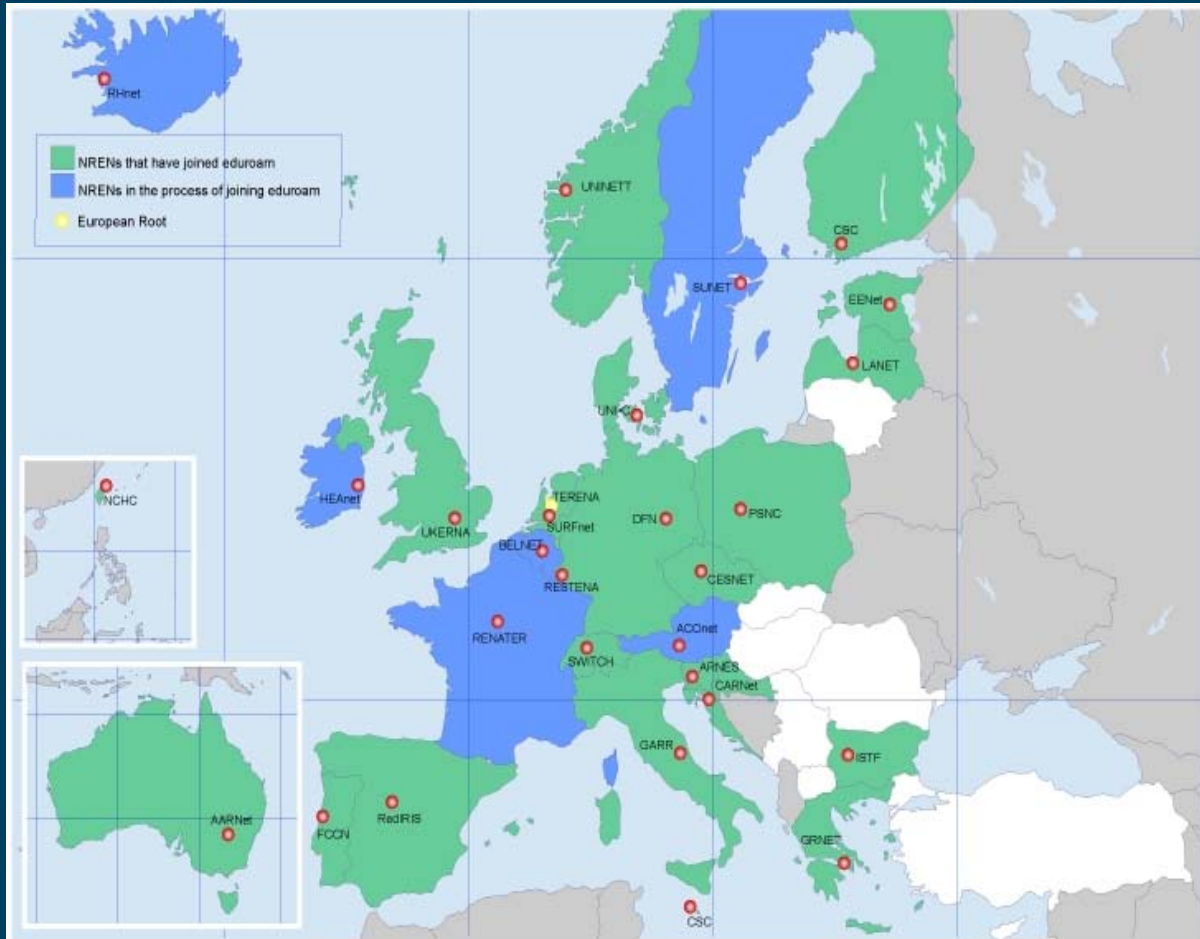
Connect. Communicate. Collaborate

- Providing roaming network access at higher education and research institutions
- Developed by TERENA taskforce on mobility (TF-Mobility)
- Pilot service started start of 2004
- JRA5 will transform the pilot service into a full service by:
 - Creating the necessary policies and governance bodies
 - Making the infrastructure more robust



Status of *eduroam*

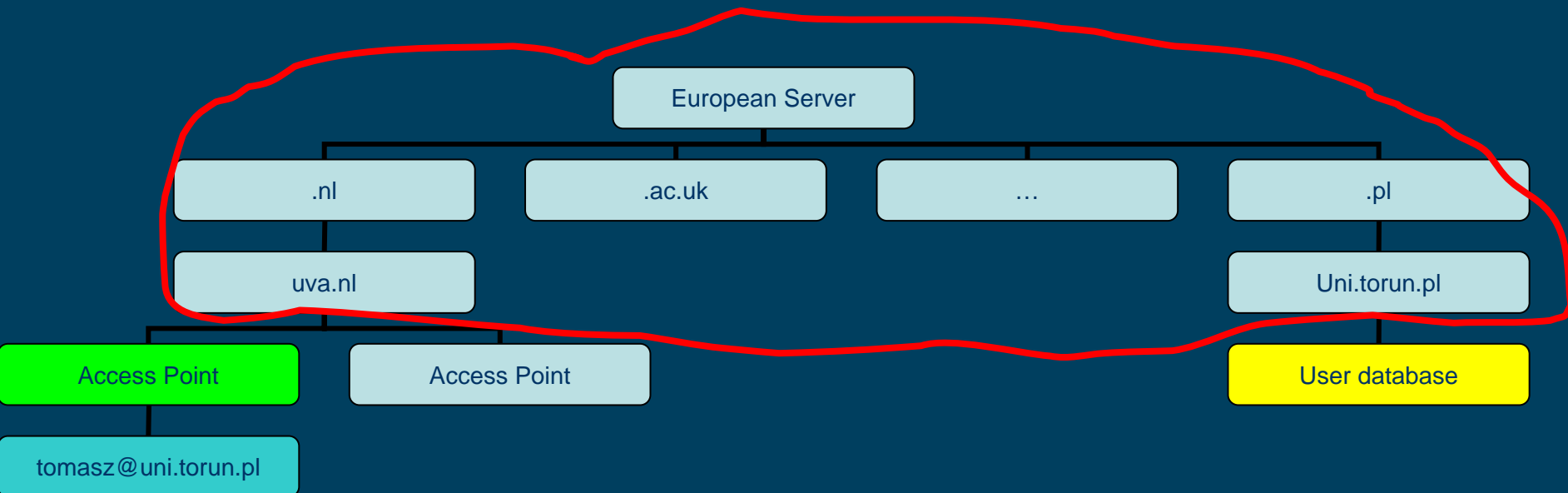
Connect. Communicate. Collaborate



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



Technology: bypassing the hierarchy overhead?



- AA traffic goes through all intermediate entries
- All links are peer-to-peer agreements / static routes / p2p secure
- DIAMETER? DNSsec? RadSec? Work on-going in Telematica Instituut/JRA5 partners

Other limitations of the current roaming infrastructure



Connect. Communicate. Collaborate

- **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?
- **eduGAIN**
 - How can we integrate roaming with the European AAI eduGAIN?



Architecture alternatives

- DIAMETER (RFC 3588)
 - Problem: no DIAMETER “quality” implementation so far
- RADIUS/DNSSec
 - Look-up through secure DNS
 - Dedicated roaming domain secure DNS tree needed
- RadSec (Radiator team)
 - Trust establishment very similar to the DIAMETER + DNS and PKI
 - Not a standard solution (yet), not all RADIUS implementations for now
 - Experimental work done



Connect. Communicate. Collaborate

Content

- Overview
- Roaming infrastructure
- **AAI**



Connect. Communicate. Collaborate

AAI Goals

- To build an interoperable authentication and authorisation infrastructure that will be used all over Europe enabling seamless sharing of e-science resources
- Basic idea: Federate and interoperate preserving existing solutions (protecting investments)
- eduGAIN is the name we have coined for this infrastructure



Connect. Communicate. Collaborate

AAI Current Activities

- Implementation phase launched and steaming to full speed
 - Documenting profiles
 - Appointed to update the architectural definition
 - Web SSO, perfSONAR...
 - Working environment being established
 - SVN server
 - Common libraries and language(s)
 - Validation suites using AA-RR
 - Task identification and assignment
 - Connectors for current federation technologies



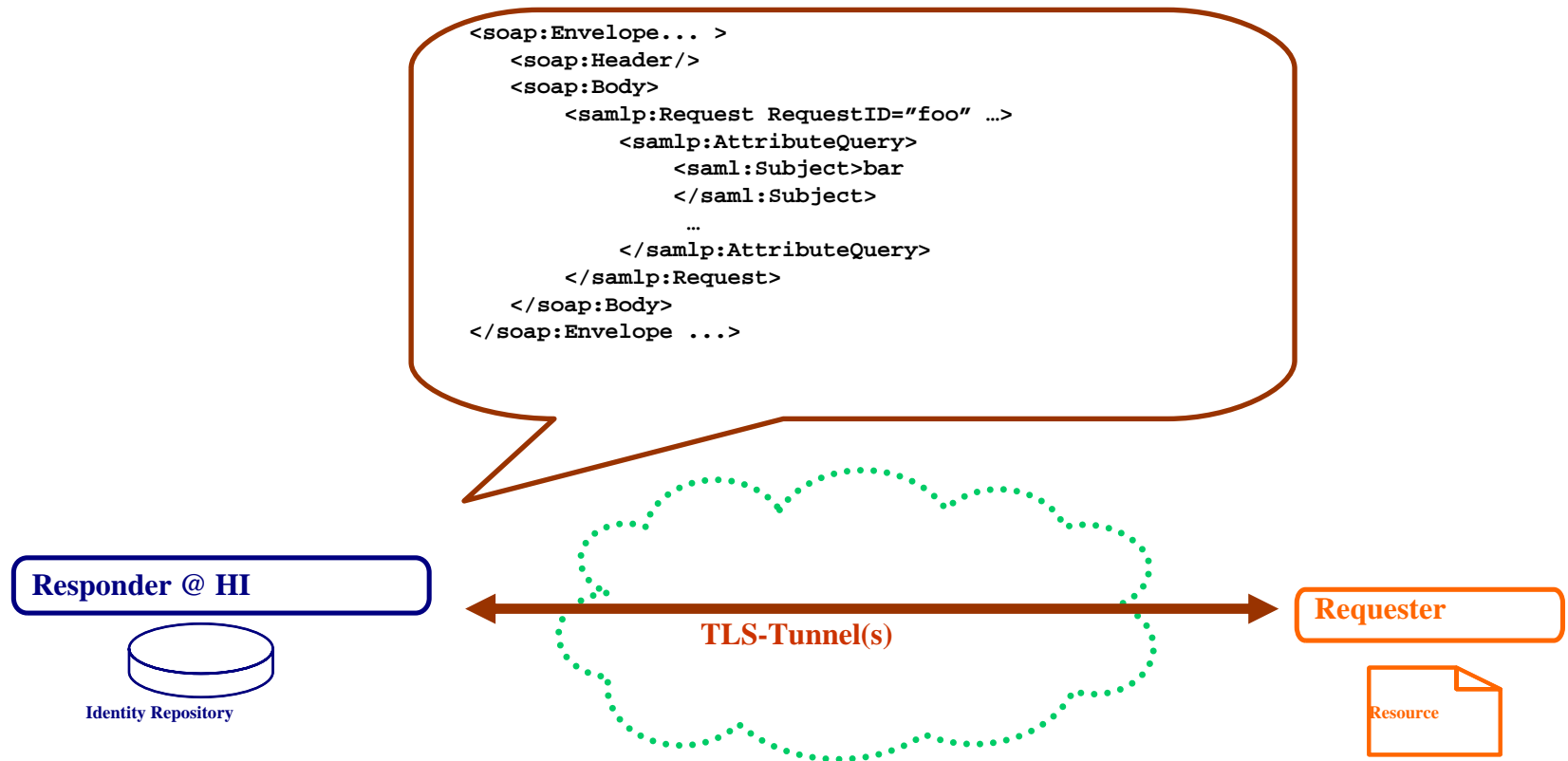
eduGAIN Operations

- Defined in abstract terms, following the SOA paradigm
 - Home Location Service (HLS)
 - Authentication Service (AuthN)
 - Attribute Exchange Service (Attr)
 - Authorisation Service (AuthZ)
- Formally defined parameters for each operation
- Bindings defined for SAML 1.1 and part of SAML 2.0
 - Plans for evolving these bindings as required
- The common eduGAIN access API will be based on this definition

A general model for eduGAIN operations



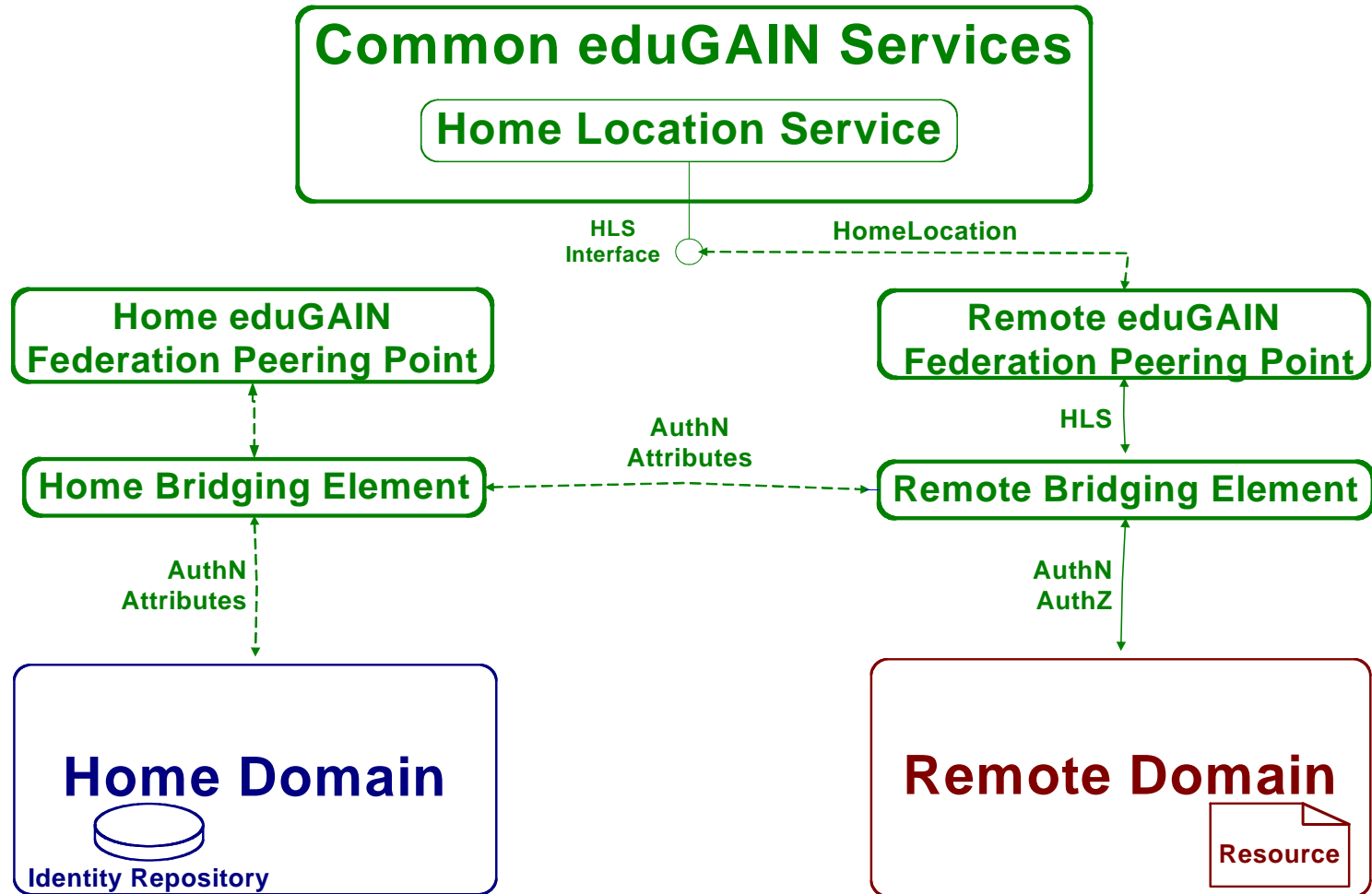
Connect. Communicate. Collaborate





eduGAIN Components

Connect. Communicate. Collaborate



eduGAIN Components: The HLS and the FPPs



Connect. Communicate. Collaborate

- FPPs establish the link between BEs, using local policies to
 - Select the appropriate interfaces
 - Provide trust material
 - Request specific features
- FPPs use the Home Location Service to query and announce interface availability and requirements
 - Queries are processed in a directory style
 - With possible redirections
 - Interfaces are announced through a publish interface
- Current binding uses SAML 2.0 metadata

eduGAIN Components: BEs and the eduGAIN-base



Connect. Communicate. Collaborate

- Bridging Elements adapt between local and eduGAIN procedures and protocols
 - Either at the federation top level: LFAs
 - Or at the local level: LAs
- The use of each BE depends on local policies
 - And can coexist
- The eduGAIN-base is the common library for all eduGAIN components
 - Direct implementation of the eduGAIN service definition
 - And also available to local requesters and responders



Connect. Communicate. Collaborate

Conclusions/Summary

- Eduroam/eduroam-ng pilot infrastructure is growing, policy will be added, roadmap for migration to service next Summer
- discussion of the new roaming architecture also with groups from Australia, USA and more partners in the global working group on eduroam (gwg).
- There are a number of national operational federations in place, and a test platform for eduGAIN will be built upon these AAls. To be set up soon.
- Support for AA integration into other GN2 activities.
- Interest is growing in both roaming and AAI worldwide

Questions please



Connect. Communicate. Collaborate



JRA5 Team

