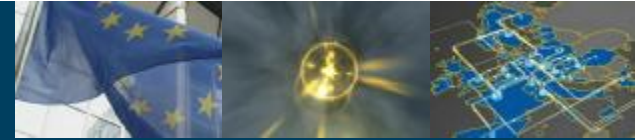


GN2 JRA5: Roaming and Authorisation

Jürgen Rauschenbach, DFN

TF-NGN Athens

03/11/05



Connect. Communicate. Collaborate

Introduction

- JRA5 builds a European Roaming Infrastructure (eduroaming) taking into account existing experience from the roaming area and provides a first (simple, but operational) federation example
- JRA5 will pilot the federated support for existent Authentication and Authorisation Infrastructures for Research and Education, this will be called eduGAIN
- In some countries federated AAs are already available, eduGAIN will be able to cooperate with them (Shibboleth, PAPI, Moria, A-Select)
- JRA5 fits into GÉANT2 project homogenously because AA solutions are needed in the GÉANT partner countries and because other activities will use JRA5 results



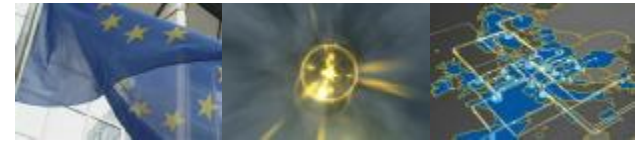


Connect. Communicate. Collaborate

Structure and Partners

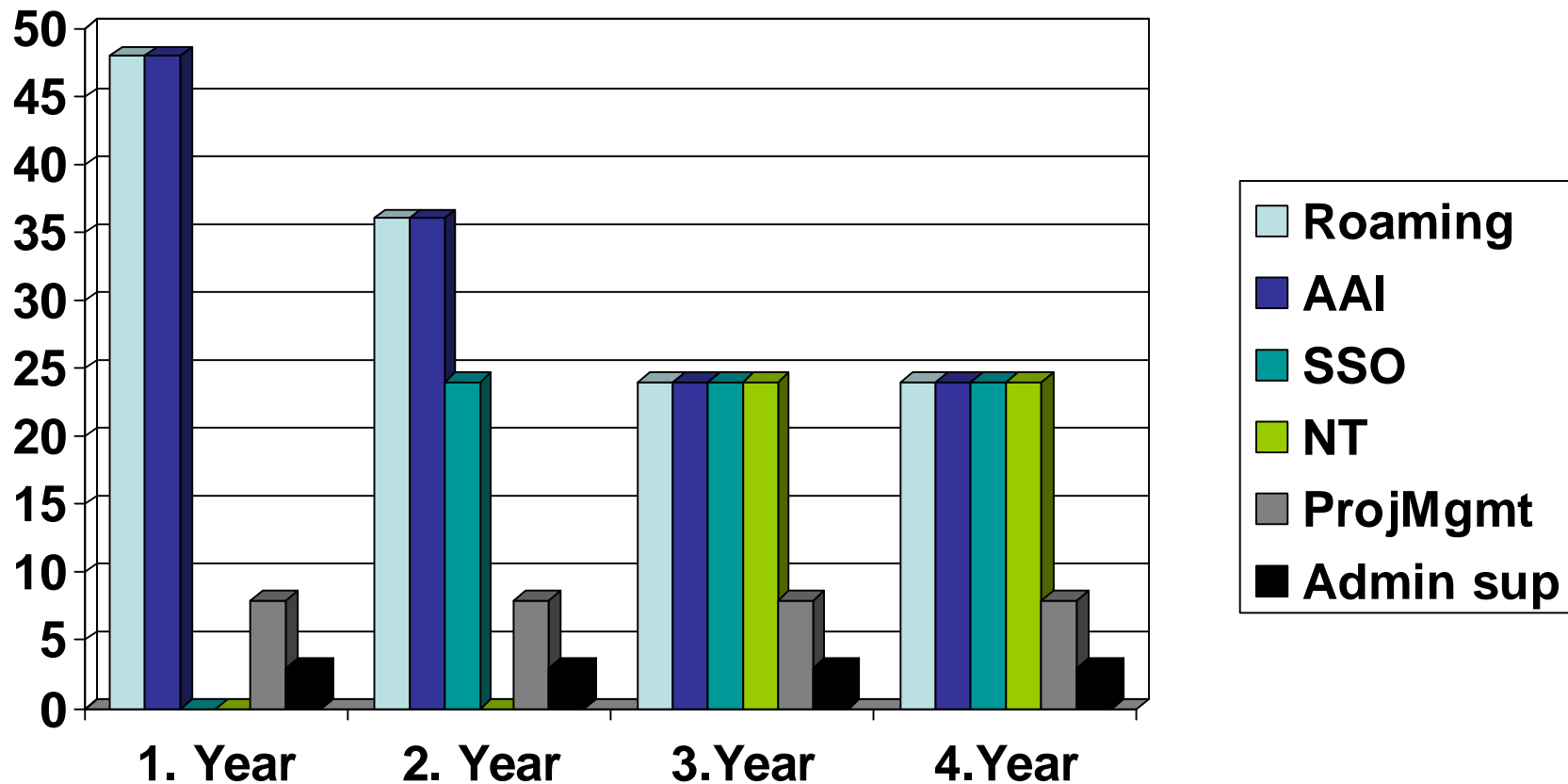
- JRA5 consists of the following Work Item in the 4 project years:
 - WI-1: Roaming
 - WI-2: Authentication and Authorisation Infrastructure
 - WI-3: Single Sign-On
 - WI-4: Integration of advanced Technologies
- Number of partners is 16 (NRENs), Number of participants is 97 (mailing list), with contributions of around 30-35 active persons
- Partners are SURFnet, DFN, RedIRIS, SWITCH, NORDUnet (University of Umea, UNI-C, UNINETT, CSC), RESTENA, ARNES, CARNET/SRCE, CESNET, FCCN, GRNET, HEAnet, HUNGARNET, ISTF, Ukerna, Dante
- Collaboration with many external groups: TF-Mobility, TF-EMC2, GN2 activities (JRA1, SA3), international groups like gwg, FWNA, Grids, ...

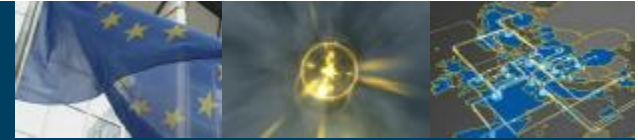




Connect. Communicate. Collaborate

Work item distribution



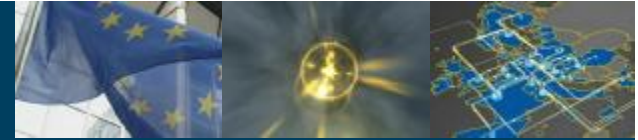


Connect. Communicate. Collaborate

Work plan first 18 months

- On our agenda (deliverables):
 - 1: Terminology for Roaming (and AAI)
 - 2: AAI Requirements
 - 3: Roaming Requirements
 - 4: Roaming policy (legal material, policy document part1 and 2)
 - 5 Design of the AAI Architecture
 - 6: Architecture of eduroam-ng
 - 7: Requirements single sign-on
- All objectives in months 1-12 have been met J





Connect. Communicate. Collaborate

Year 1 - Achievements

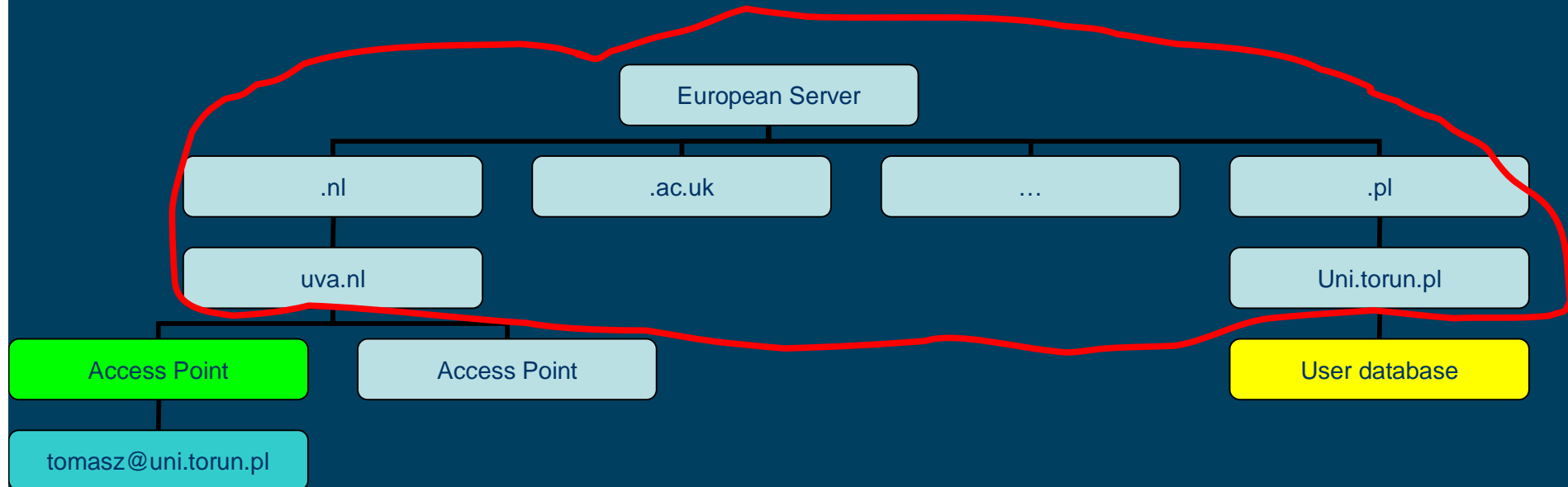
- Work item 1 Roaming
 - A-1: “Glossary of Terms” [DJ5.1.1](#), a terminology document, scope roaming and AAI, to be extended with new terms
 - A-2: was the “Roaming Requirements document” [DJ5.1.2](#); security, standardisation and operational aspects
 - A-3: have been contributions to the extension of the roaming pilot “eduroam”, both in the number of participants (NRENs) and also functionally (analysing the current infrastructure, eduroam-in-a-box, alternative architecture discussion).
 - A-4: co-operational work with the TF Mobility, use eduroam as experimental platform in JRA5 as a step stone to eduroam-ng. Open discussion and dissemination on the mobility list.
 - A-5: “legislation overview” for roaming services. [DJ5.1.3-1](#) federation policy is currently in an early draft state. [DJ5.1.3-2](#)





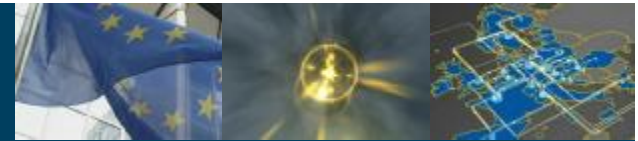
Connect. Communicate. Collaborate

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? Work on-going in Telematica/JRA5 partners

Limitations of the current roaming infrastructure



Connect. Communicate. Collaborate

- **Technology**
 - All authN and authZ traffic flows through the complete hierarchy
 - Static trust (shared secrets in preconfigured p2p chain)
 - Single points of failure (even when doubling the top level RADIUS)
- **Policy**
 - Not suitable for full service yet
- **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?



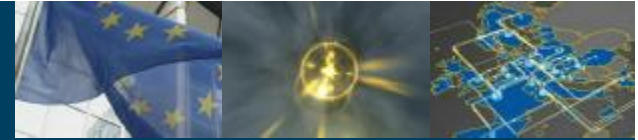


Connect. Communicate. Collaborate

Architecture alternatives

- DIAMETER (RFC 3588)
 - Protocol defines different routing models to find the peer (redirect agent, redirect + PKI, DNS NAPTR/SRV + PKI)
 - For inter-domain DNS based model looks promising
 - DNSSec would be an alternative here (not part of the standard)
 - Integration with “legacy” RADIUS by translation agents, gradual transition would be possible, but RADIUS have to stay
 - Problem: no DIAMETER “quality” implementation so far
- RadSec (Radiator team)
 - Trust establishment very similar to the DIAMETER + DNS and PKI
 - Not a standard solution, not all RADIUS implementations
 - Experimental work has started





Connect. Communicate. Collaborate

Architecture alternatives (2)

- RADIUS/DNSSec
 - Look-up through secure DNS
 - Visiting RADIUS establishes a TLS connection to the home RADIUS to negotiate a shared secret (RKE protocol): dynamic p2pconnectivity
 - Then it works like a normal RADIUS connection
 - Dedicated roaming domain secure DNS tree needed
- RADDNSSEC
 - Modified RADIUS/DNSSec, TLS handshake instead of RKE
- No smooth and easy deployment for the alternatives
- DIAMETER ranks high, but RadSec seems to be available faster

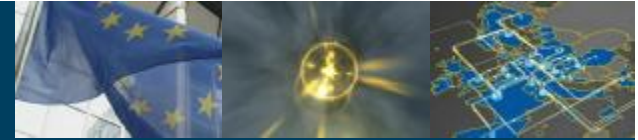
Year 1 – Achievements (2)



Connect. Communicate. Collaborate

- Work item 2 AAI
 - A-6: “AAI Requirements document” **DJ5.2.1** setting the scope of an AAI solution and defining first building blocks and general federation functionality, illustrated in examples and use cases
 - A-7: AAI architecture document **DJ5.2.2** (published last week)
- Work item 3 SSO
 - No real work done so far



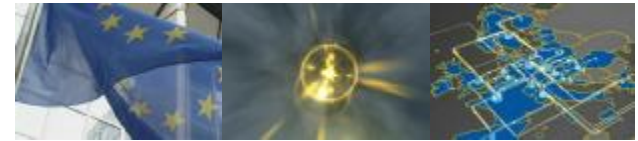


Connect. Communicate. Collaborate

AAI operations

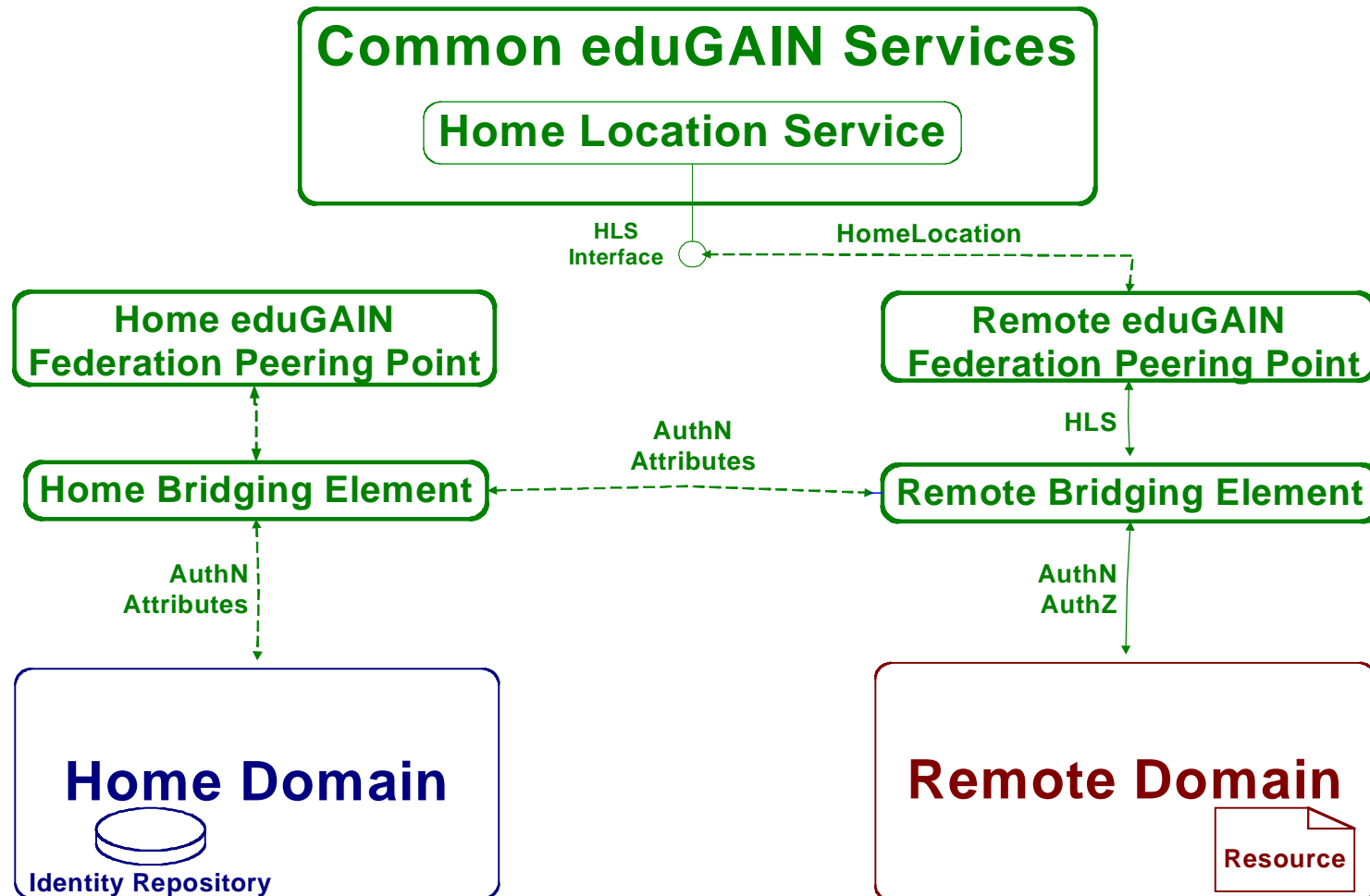
- Authentication request
- Authentication response
- HLS request
- HLS response
- Attribute request
- Attribute response
- Authorisation request
- Authorisation response
- Operations formally defined (SAML 1.1), openSAML for implementation (SAML 2.0 is announced already)
- Web services (WS) context

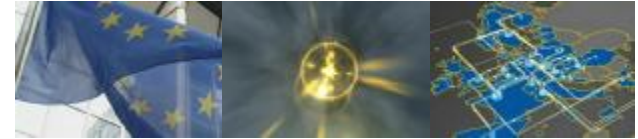




Connect. Communicate. Collaborate

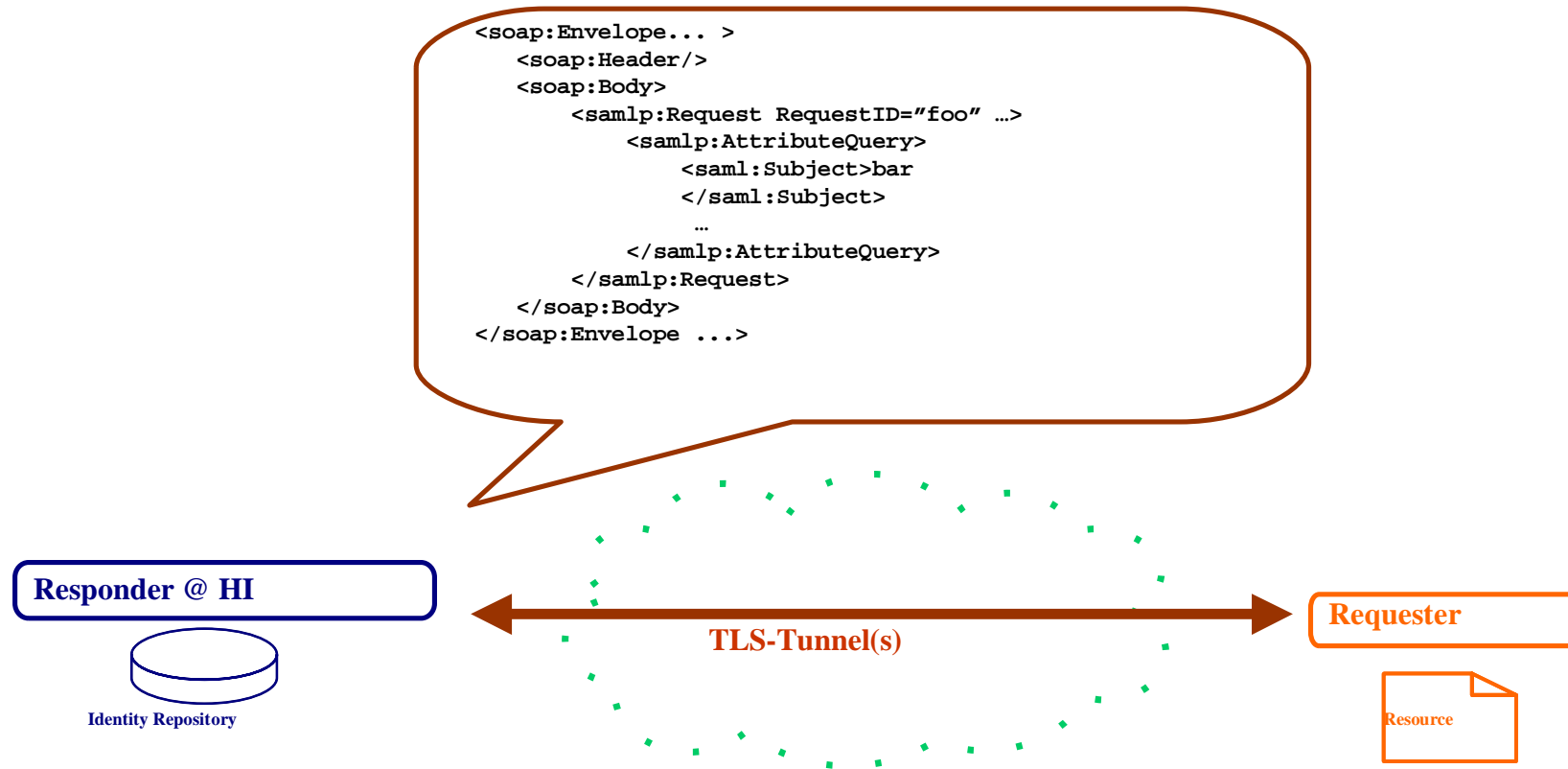
AAI – basic components

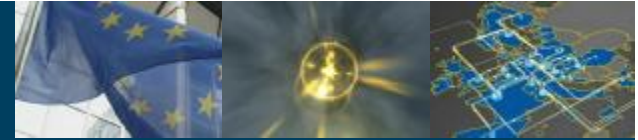




Connect. Communicate. Collaborate

Abstract AAI operation





Connect. Communicate. Collaborate

Conclusions/Summary

- Eduroam pilot infrastructure is growing into eduroam-ng, discussion of the new architecture also with groups from Australia, USA and more partners in the global working group on eduroam.
- 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 in the coming months.
- Interest is growing in both roaming and AAI
- work is not easy, but a lot of fun

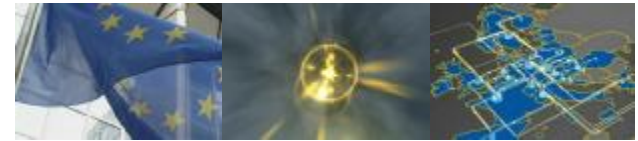




Connect. Communicate. Collaborate

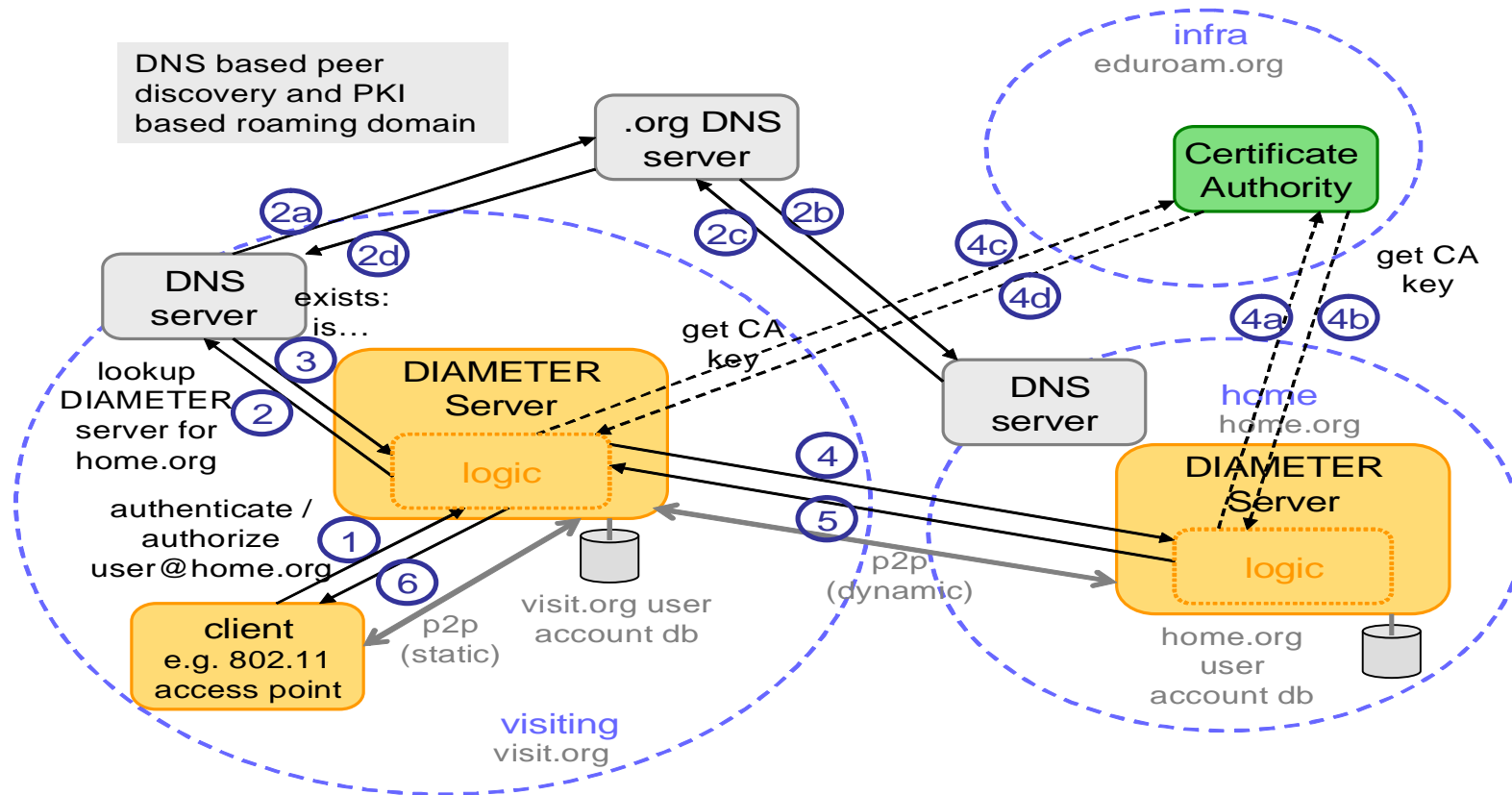
?

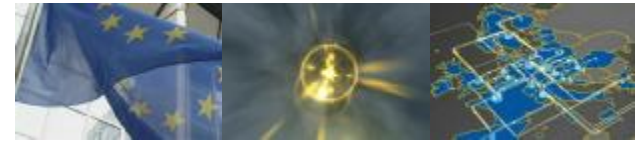




Connect. Communicate. Collaborate

DIAMETER with DNS, CA

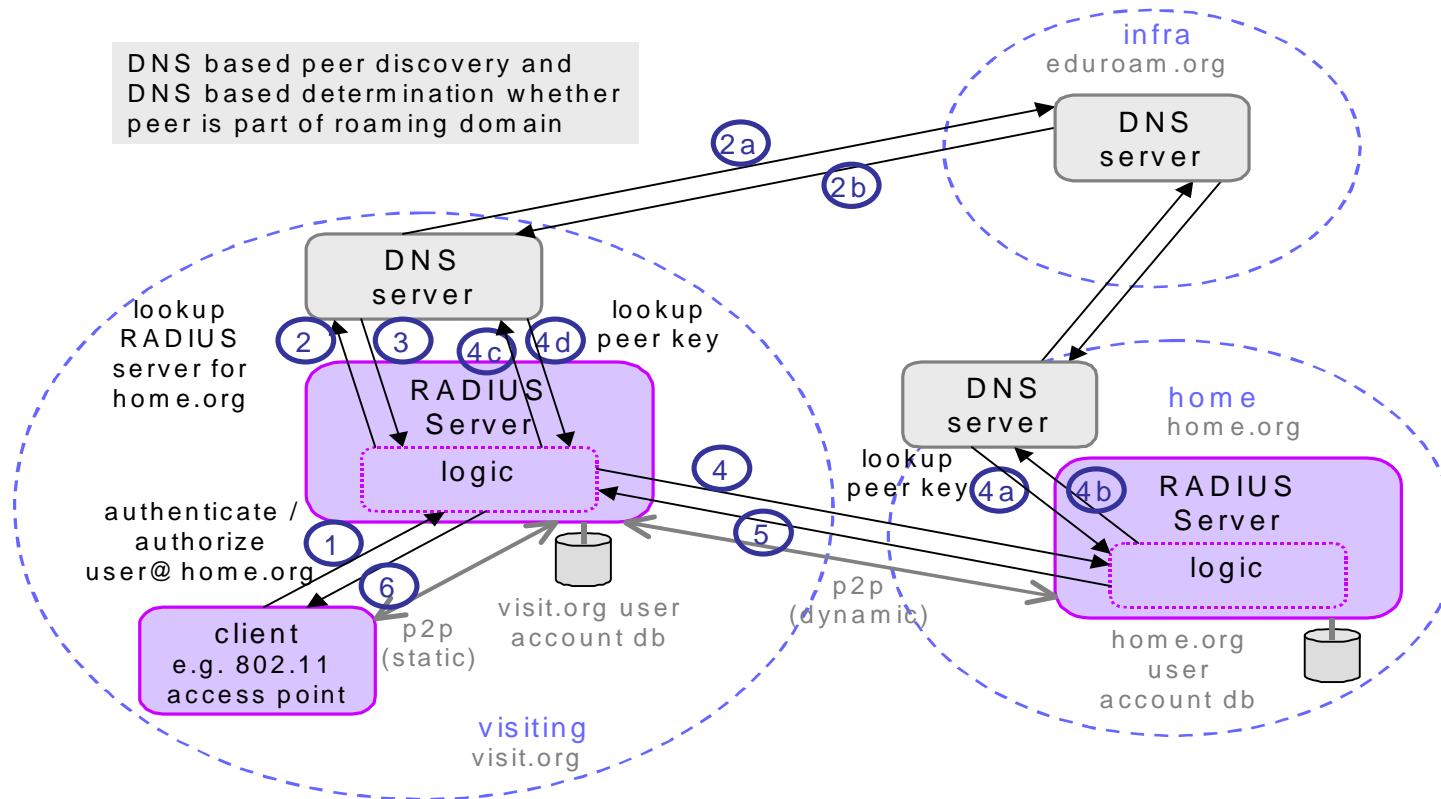




Connect. Communicate. Collaborate

RADIUS + DNSSec

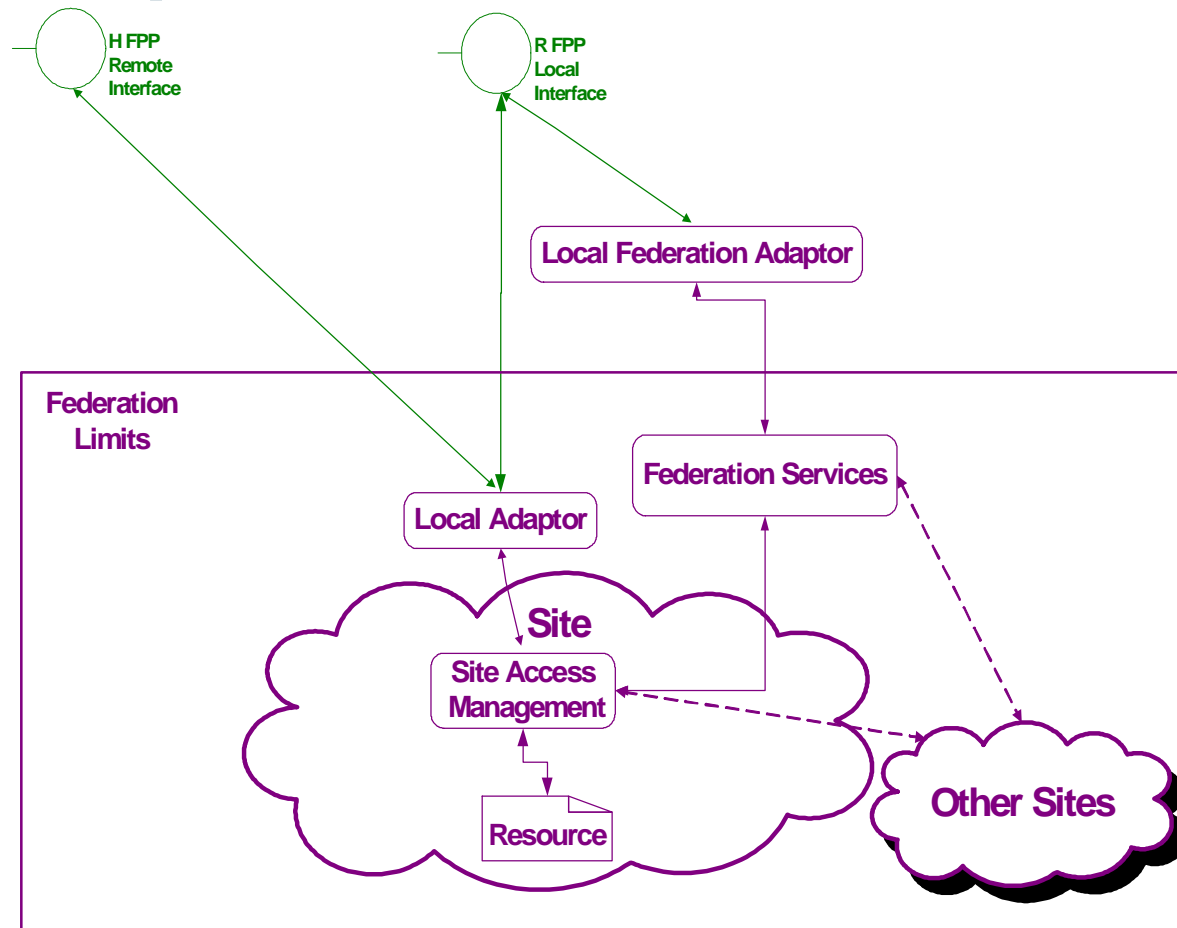
DNS based peer discovery and
DNS based determination whether
peer is part of roaming domain



Additional slide: AAI – components LFA/LA



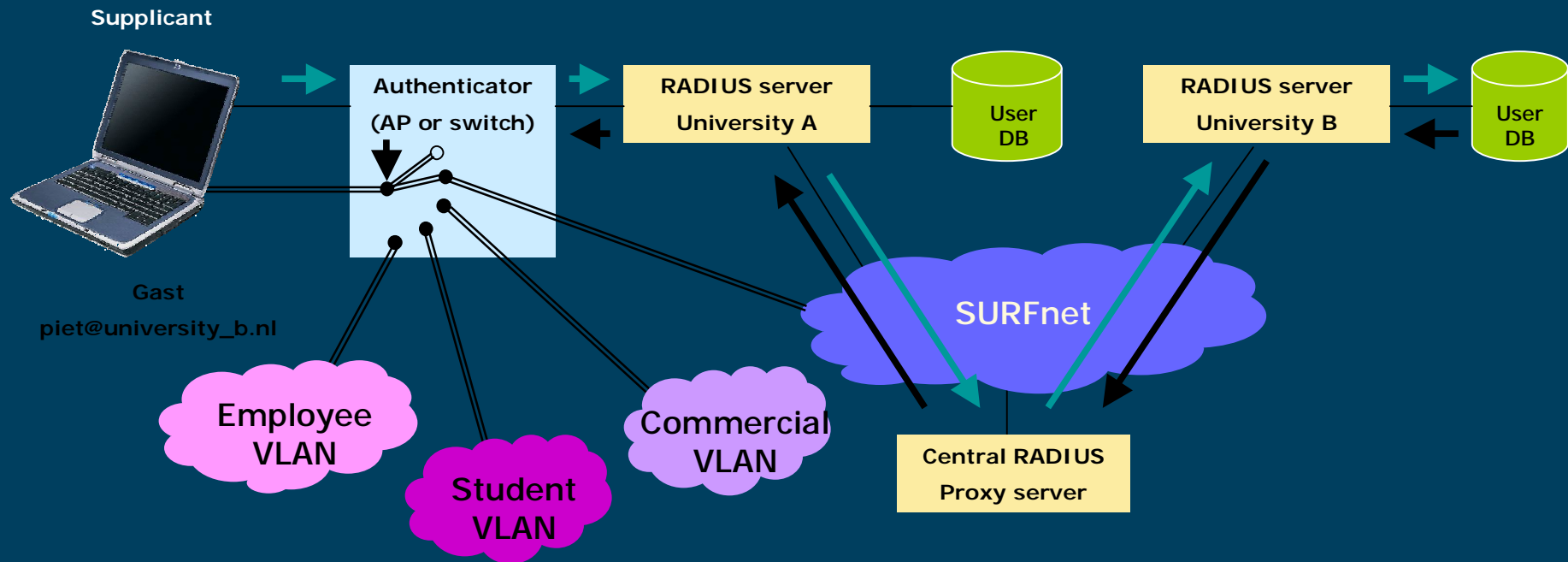
Connect. Communicate. Collaborate



EduRoam



Connect. Communicate. Collaborate



→ signaling
 == data

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

