



Towards eduroam-NG in Europe: Overview and Comparison of Advanced Roaming Protocols

Henk.Eertink[§], Arjan.Peddemors[§], Remco.
Poortinga[§], Roy Arends[†], Klaas.Wierenga[‡]

[§]@telin.nl [†]roy@dnss.ec [‡]@surfnet.nl

TNC 2006, Catania, May 17 2006



Connect. Communicate. Collaborate

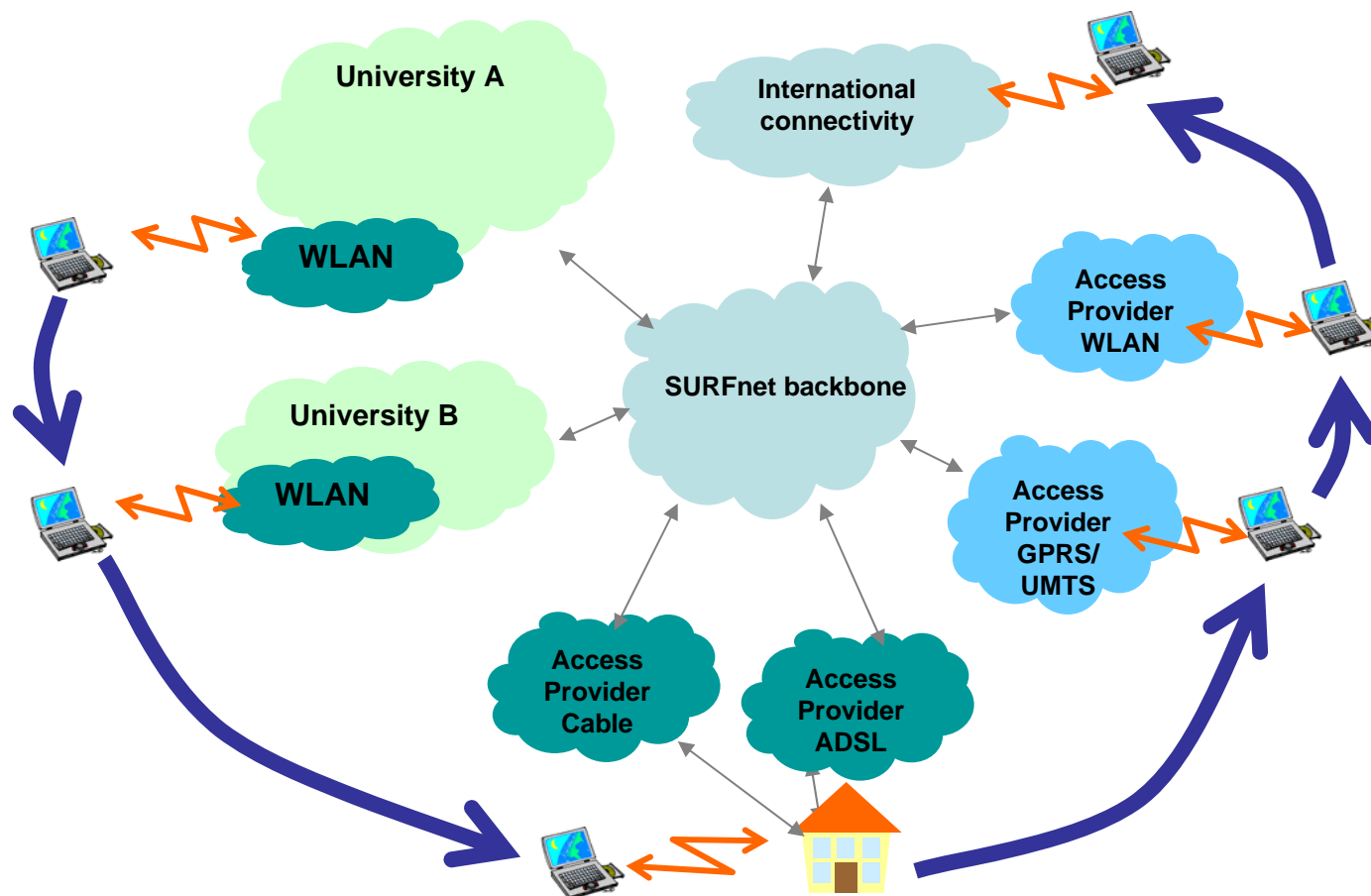
What are we talking about?

- Roaming in *eduroam*
- Requirements for *eduroam*-NG
- Protocol architectures for roaming
- Deployment scenarios in Geant2
- Test and Evaluation results

eduroam: supporting your mobile users

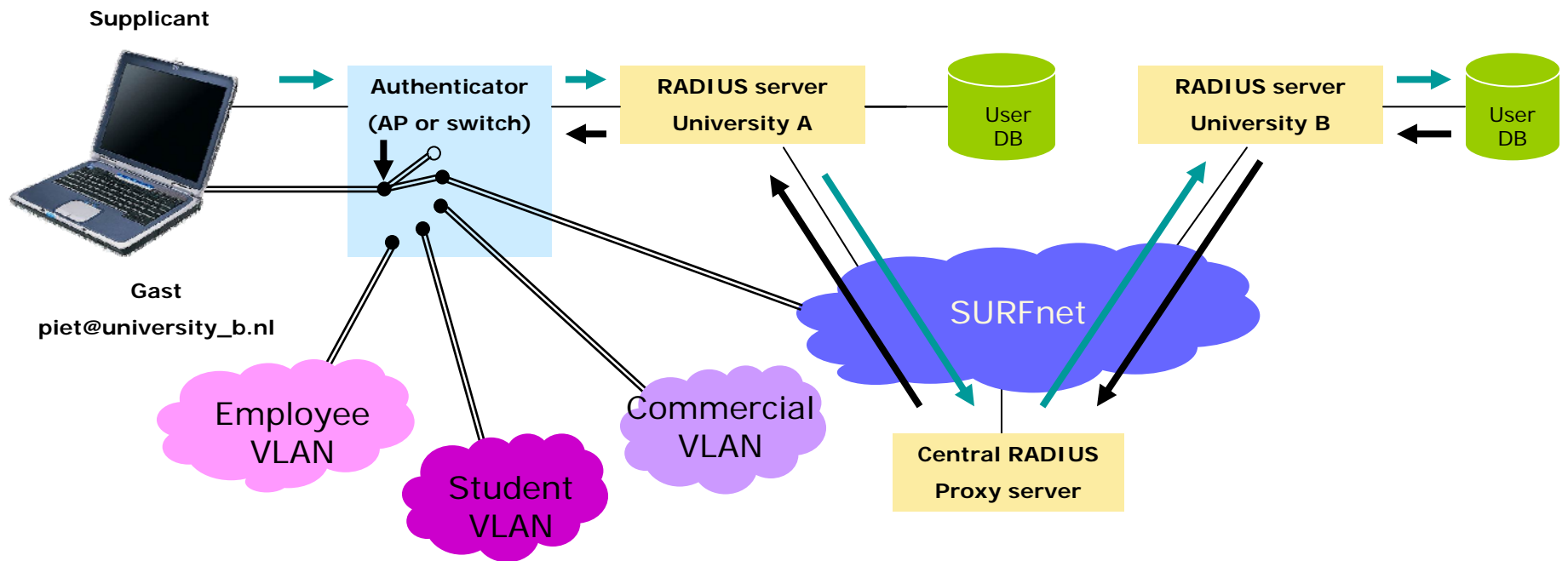


Connect. Communicate. Collaborate



eduroam internals

Connect. Communicate. Collaborate



Gast
piet@university_b.nl

→ signalling
== data

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



Status of *eduroam*

Connect. Communicate. Collaborate



New members:

- Lithuania
- Romania
- Hungary
- USA

Japan, Korea, Hong Kong, China will follow shortly



Connect. Communicate. Collaborate

eduroam-NG: Requirements

- GEANT2 roaming facility = eduroam-NG
- Downward compatible with existing eduroam (RADIUS, 802.1X) ←
- Intended key improvements of eduroam-ng ←
 - Dynamic trust establishment ←
 - More formally defined form of federation
 - Integrated 802.11i and WPA/WPA2
 - Scalability and monitoring ←
 - Attribute-based authorization

Requirements as taken from GEANT2 deliverable DJ5.1.2:
“Documentation on the GEANT2 Roaming Requirements”

'Dynamic Trust Establishment' and 'Scalability'



Connect. Communicate. Collaborate

- *Dynamic Trust Establishment* and *Scalability* requirements typically translate into
 - Direct connections between parties (peers) involved in handling an authentication / authorization request
 - No RADIUS tree traversing as with current eduroam setup
 - But, peers **do not** have a **direct** formal relationship
- Connection setup between peers consists of two steps
 - 1) Peer discovery (Which server handles authentication / authorization requests for the user's realm?)
 - 2) Confirm that peer (or user realm) is part of roaming domain (Is the user part of the community that shares resources?)

'Peer Discovery' and 'Roaming Domain Participation'



Connect. Communicate. Collaborate

Common setup for protocols

- Peer discovery
 - DNS based
- Confirmation of participation in roaming domain
 - Public Key Infrastructure (PKI) based
 - DNS based (using secure extensions)

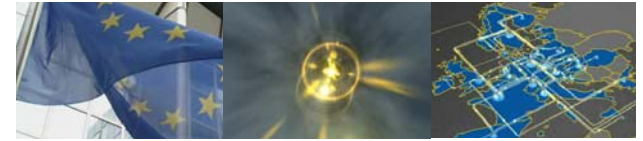
Protocol architectures for roaming



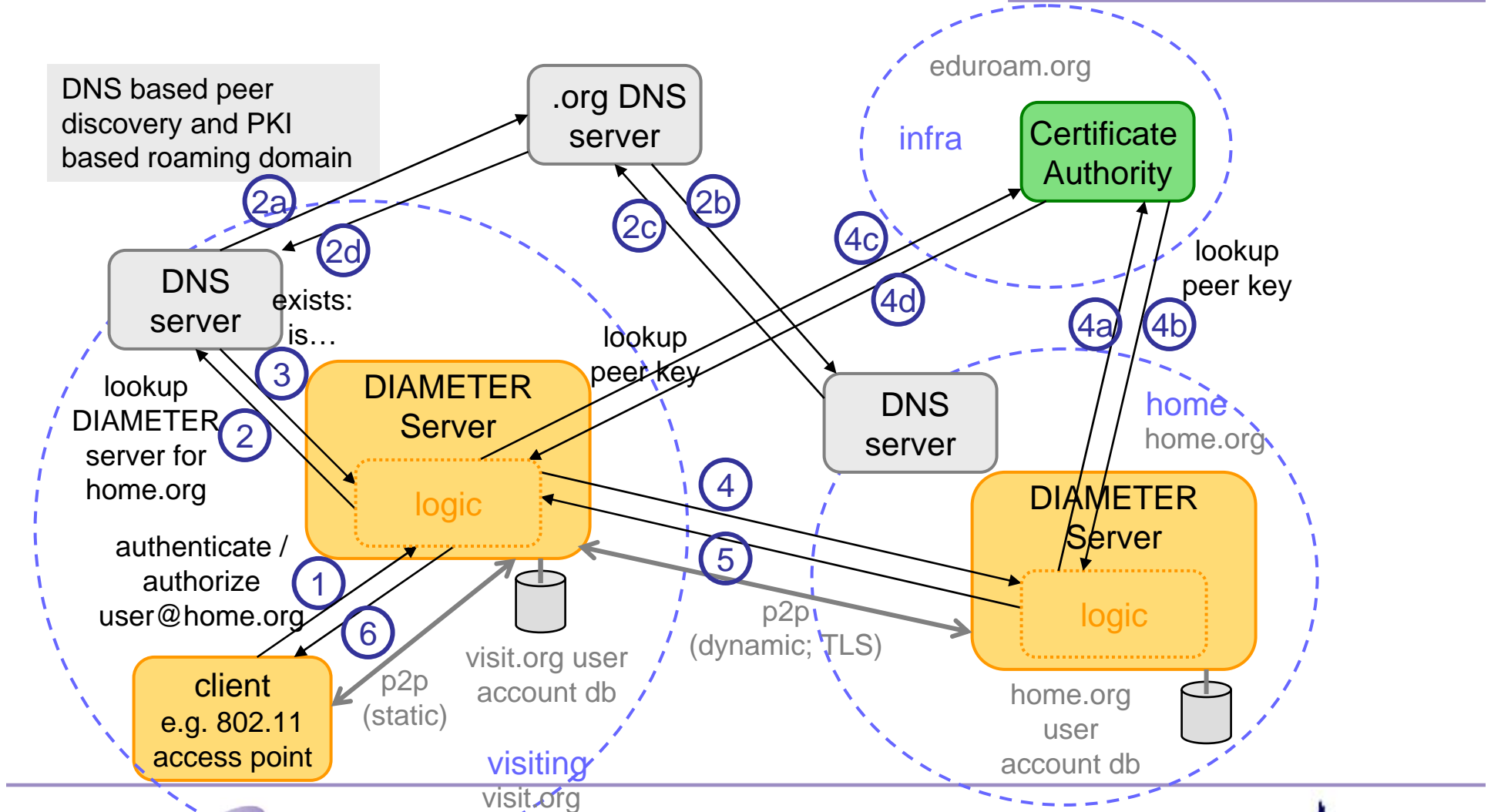
Connect. Communicate. Collaborate

- 3 architectures have been analysed:
 - Diameter. IETF defined this as successor for RADIUS
 - P2P Radius
 - Trust based on dnssec (radius-dnssec)
 - Trust based on PKI (RadSec)

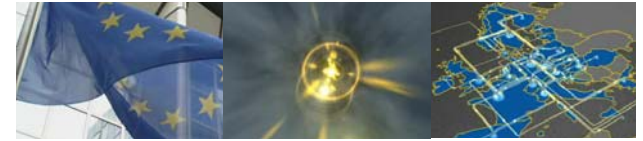
DIAMETER



Connect. Communicate. Collaborate

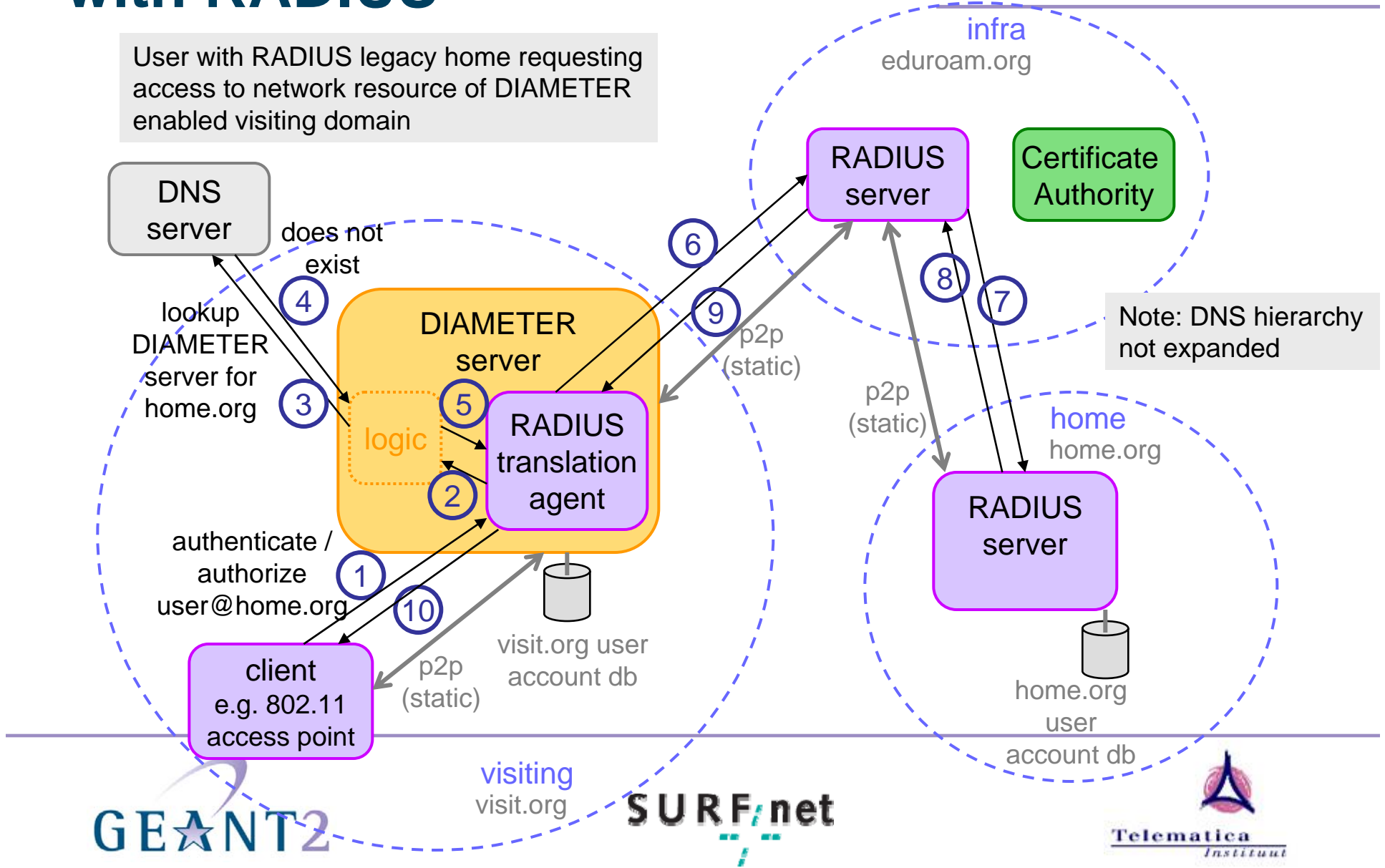


DIAMETER combined with RADIUS



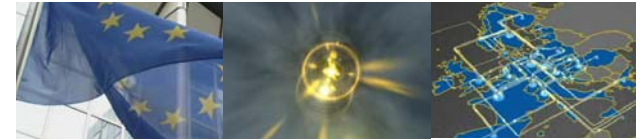
Connect. Communicate. Collaborate

User with RADIUS legacy home requesting access to network resource of DIAMETER enabled visiting domain



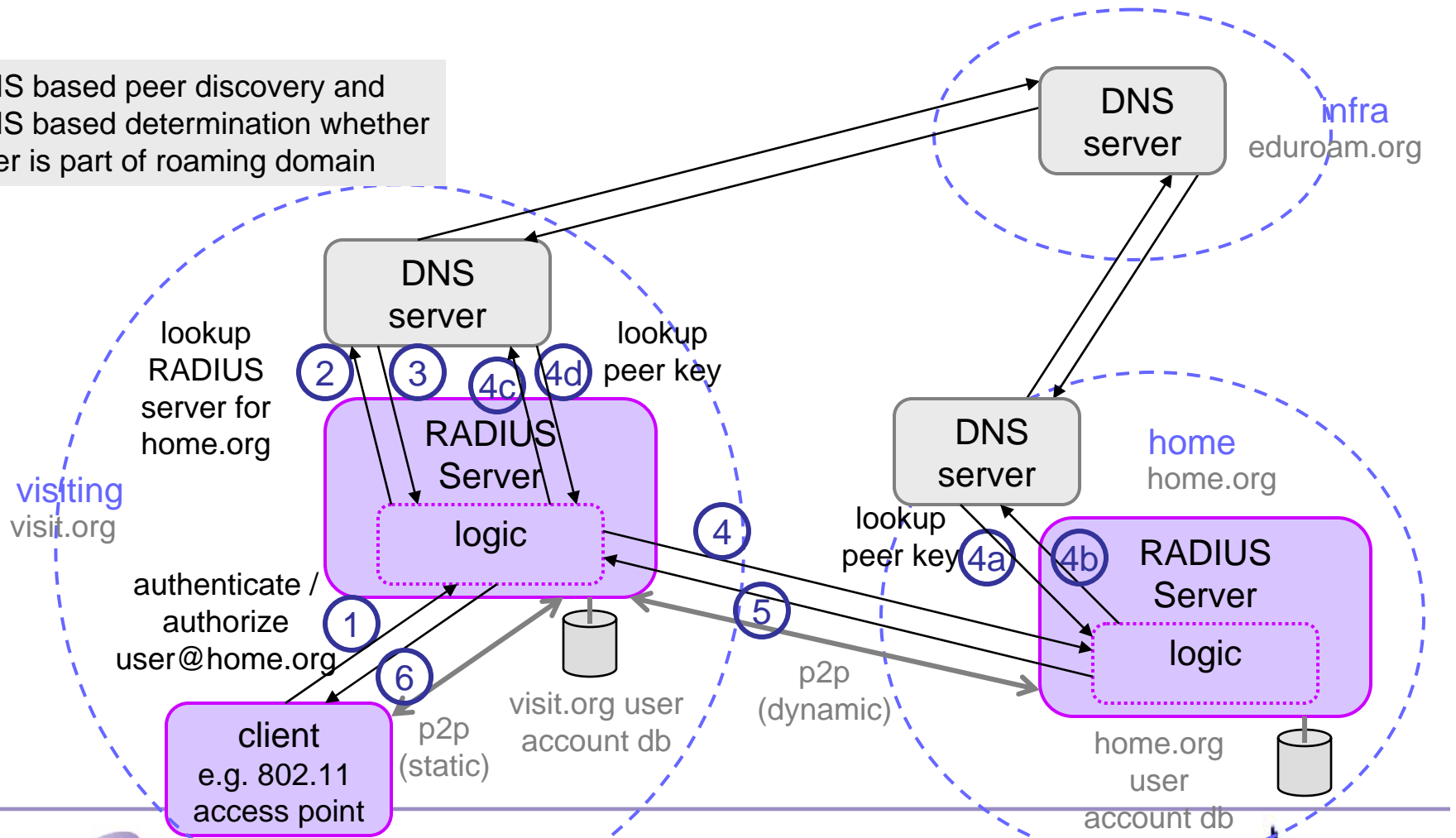
Note: DNS hierarchy not expanded

radius-DNSsec (our paper in TNC2005)

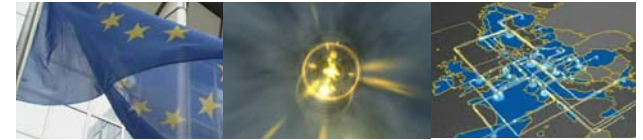


Connect. Communicate. Collaborate

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

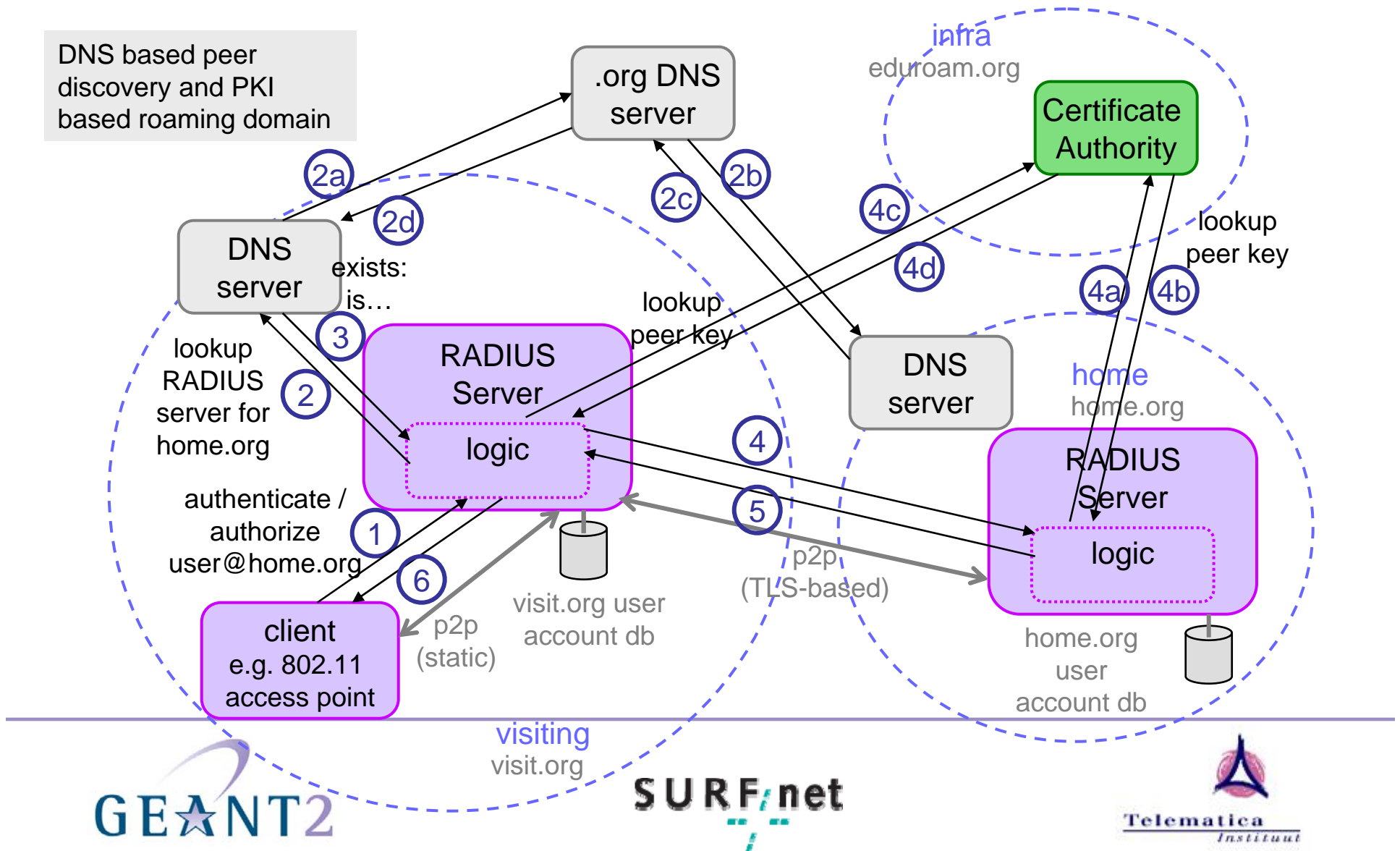


RadSec / DNSROAM (OSC Radiator extension)



Connect. Communicate. Collaborate

DNS based peer discovery and PKI based roaming domain



Protocol Architectures Compared



Connect. Communicate. Collaborate

DIAMETER

1. Trust based on preconfigured set of roaming **CAs** (PKI)
2. Multiple roaming agreements? Select proper certificate.
3. No insight in membership
4. Supports migration scenarios (through translation agents)
5. Requires **PKI** management (for all organisations)
6. **Standard** usage of TLS and ipsec

RADIUS-DNSSEC

1. Trust based on pre-configured set of roaming **DNS domains**
2. Multiple roaming agreements? Select proper DNS domain.
3. Insight in membership
4. Supports migration scenarios based on fall-through RADIUS config
5. Requires **DNSsec** key management (for at least 1 organisation)
6. **Requires** an **proprietary** key-establishment protocol

RadSec / DNSROAM

1. Trust based on preconfigured set of roaming **CAs** (PKI)
2. Multiple roaming agreements? Select proper certificate.
3. No insight in membership
4. Supports migration scenarios based on fall-through RADIUS config
5. Requires **PKI** management (for all organisations)
6. **Proprietary** usage of TLS

Deployment scenarios in Geant2



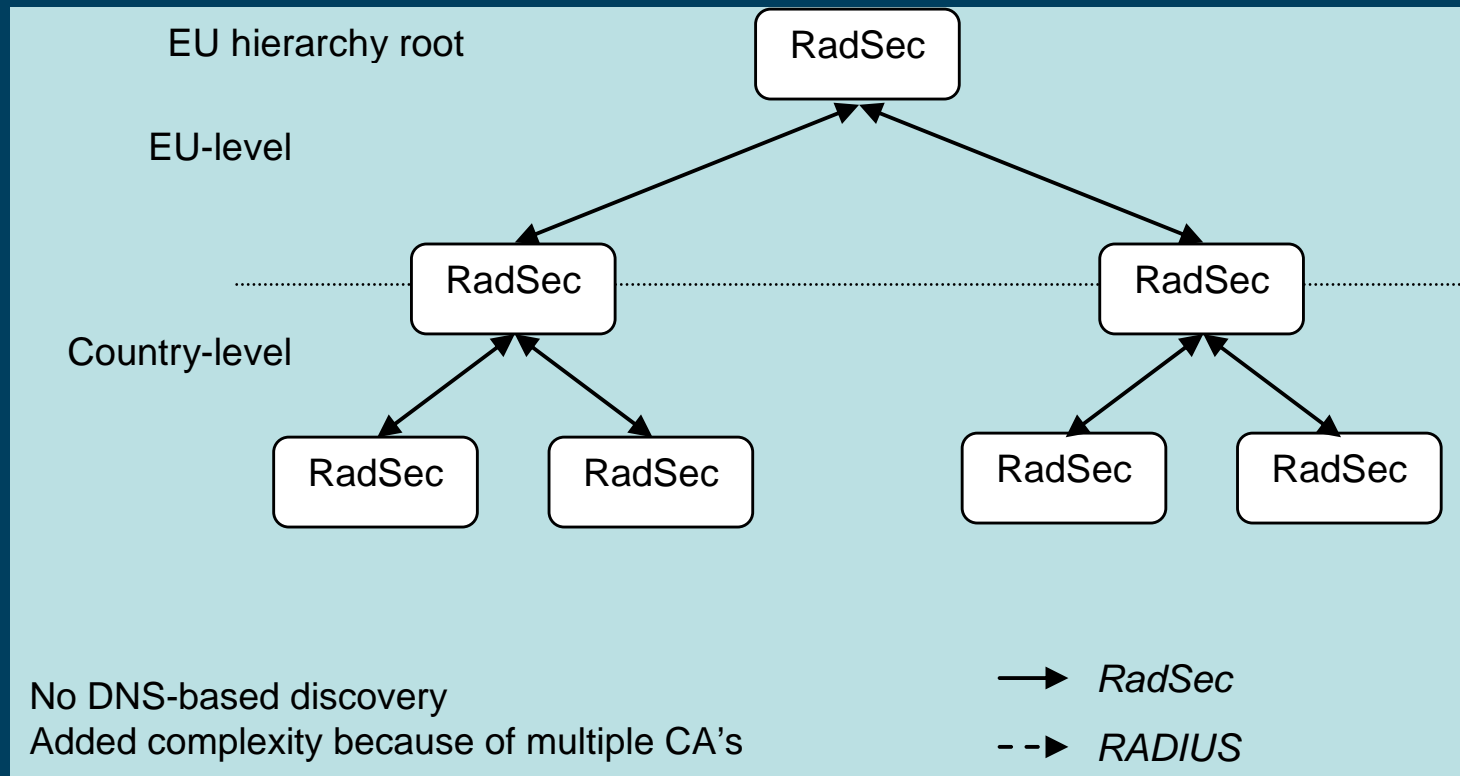
Connect. Communicate. Collaborate

- We tested the RadSec approach
 - No need for dnssec deployment
 - Somehow it backports key innovation features from Diameter to RADIUS; makes integration easier
- Multiple deployment scenarios have been studied. We describe the three that are tested:
 - Fully hierarchical
 - Meshed top-level
 - Fully meshed



Connect. Communicate. Collaborate

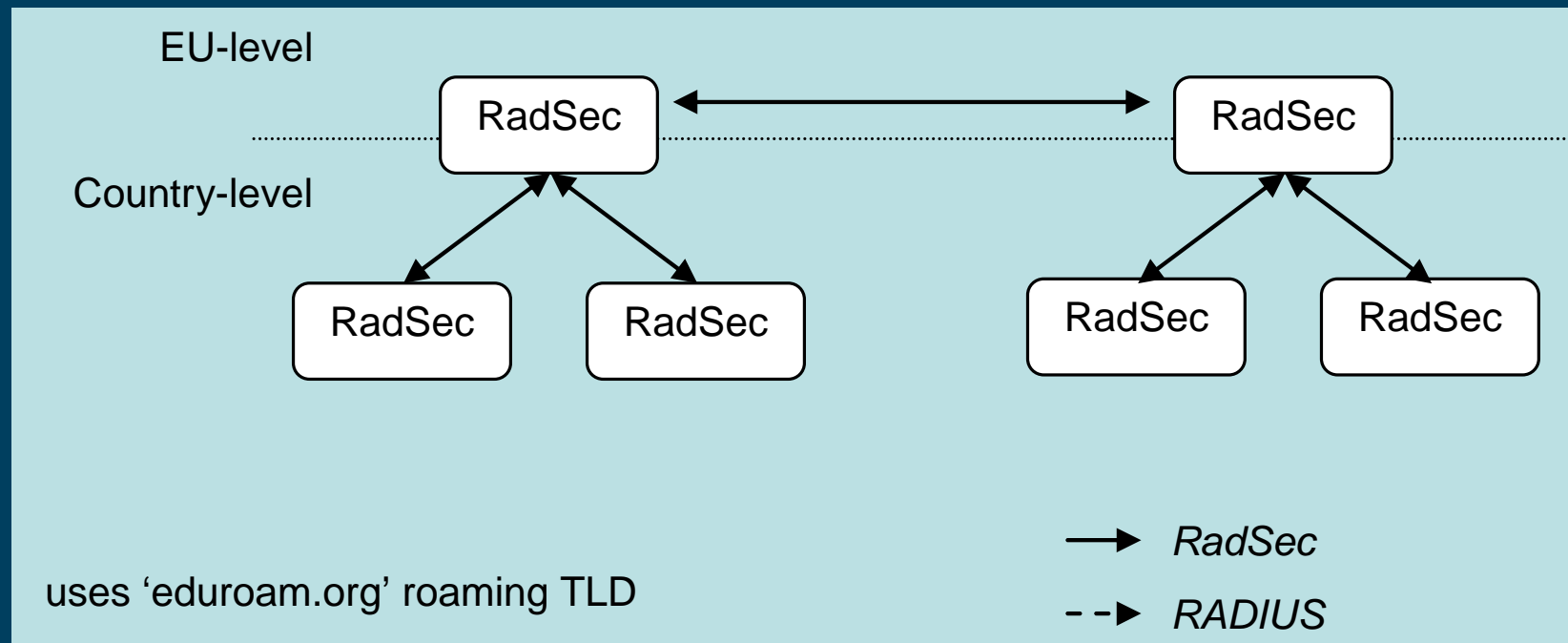
Fully hierarchical





Connect. Communicate. Collaborate

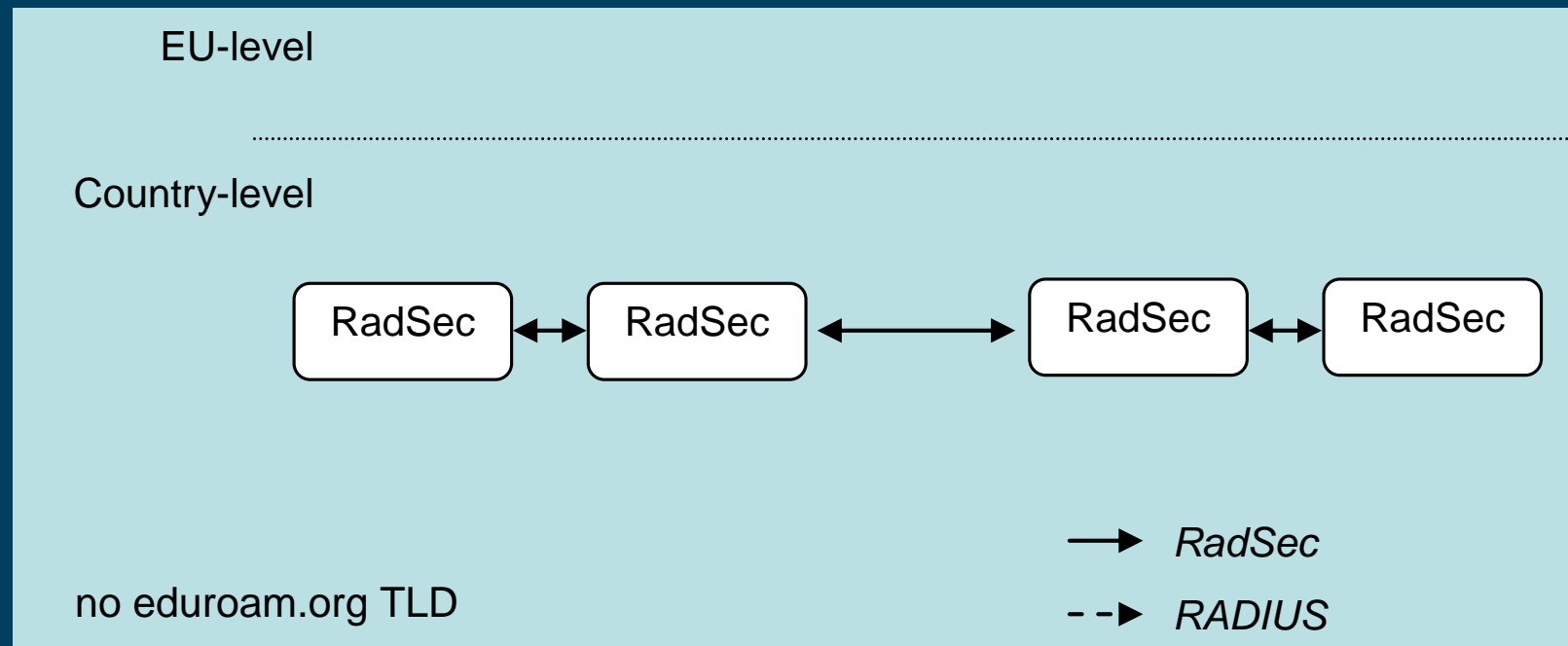
Meshed top-level





Connect. Communicate. Collaborate

Fully meshed





Connect. Communicate. Collaborate

Test and evaluation results

- Test setup
 - 6 NRENs and a number of institutions participated (SURFnet, CESNET, ISTF, TELIN, ARNES, ACAD, UNINETT, RESTENA)
 - Each scenario was tried-out between a couple of sites, and subsequently extended to a larger group
- Tested a number of cases
 - Authentication related (known/unknown user, wrong credentials)
 - PKI related (unknown CA, multiple CA, Revocation, mismatch between peer name and CN)
 - DNS related (NAPTR/SRV lookup failure, fallback)
 - Configuration related (CA cert not installed, loops)
 - Connectivity related (peer unreachable)
 - Performance related (DNS overhead)



Connect. Communicate. Collaborate

Test results

- Hierarchical scenario
 - TCP/TLS was preferred over current RADIUS (better failure detection)
 - Most appreciated scenario! (Rating: 8.2 of 10)
- Meshed top-level
 - Test used a centralized zone (test.eduroam.org)
 - 2/3 say 'DNS-based roaming is a GOOD thing'
 - 1/3: Buggy DNS-servers, DNS not secure
 - Rating: 6.2 of 10
- Fully meshed (no toplevel CA!)
 - PKI management wasn't easy (re-distribution issues and problems with revocation lists, multiple roaming configs pose problems)
 - Main issue: Auth Server has to be opened to the whole world (even though certificates are checked)
 - Score: 6.8 out of 10



Connect. Communicate. Collaborate

Conclusions

- Presented some alternatives to the current eduroam (authentication) architecture
- We obtained positive experiences in upgrading the static Radius hierarchy with the (proprietary) RadSec solution. RadSec proved (in the end) to be sufficiently stable.
- Diameter features like TLS over TCP proved useful over the current UDP-configuration of RADIUS
- Dynamic peer discovery needs more testing and consideration. This is probably more a policy issue than a technological one.



Connect. Communicate. Collaborate

THANK YOU

Henk.Eertink@telin.nl





(Nice Nagios picture)

Connect. Communicate. Collaborate

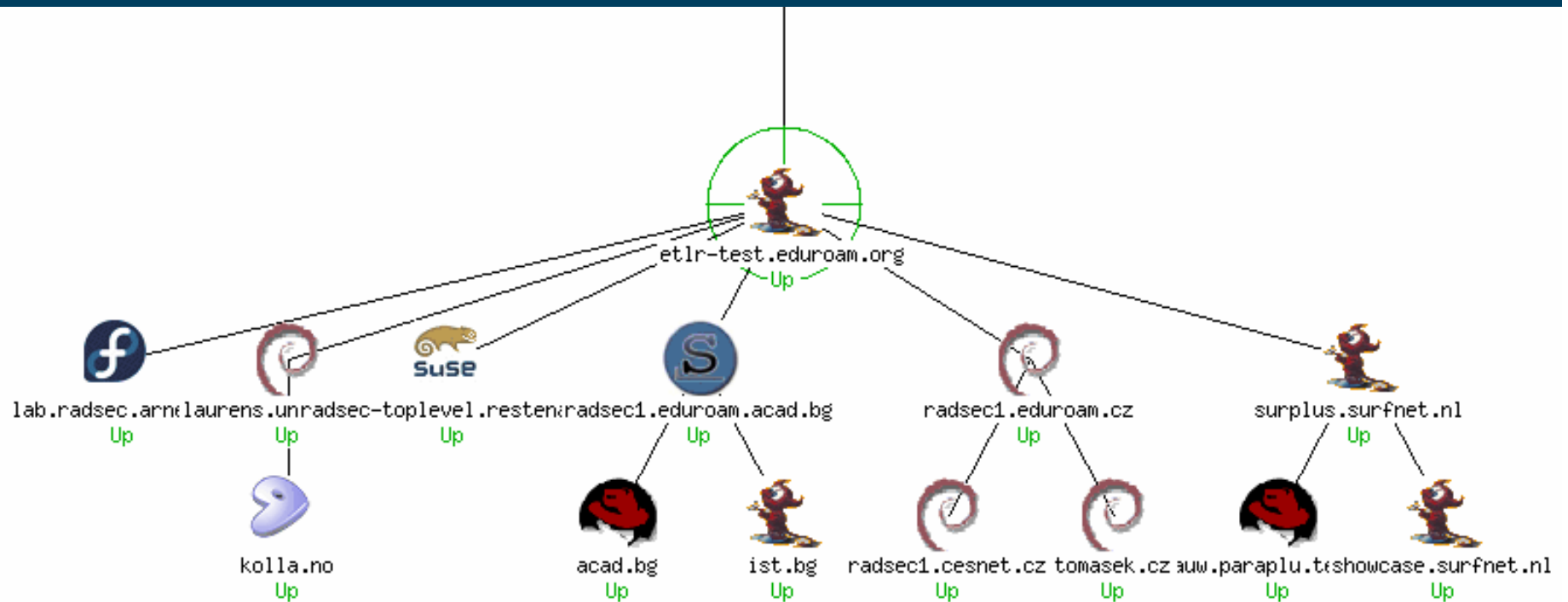


Image last updated: 12-08-2005 09:40:00

Click on the image for a circular view.



And host status

Connect. Communicate. Collaborate

realm:	last checked:	status:
acad.bg	Thu Dec 8 09:40:10 2005	OK - Access-Accept (0 attributes returned in 0.0s)
blauw.paraphu.telin.nl	Thu Dec 8 09:40:10 2005	OK - Access-Accept (6 attributes returned in 0.0s)
etr-test.eduroam.org	Thu Dec 8 09:40:10 2005	OK - Access-Accept (0 attributes returned in 0.0s)
ist.bg	Thu Dec 8 09:40:10 2005	OK - Access-Accept (0 attributes returned in 1.0s)
kolla.no	Thu Dec 8 09:39:35 2005	OK - Access-Accept (0 attributes returned in 0.0s)
lab.radsec.arnes.si	Thu Dec 8 09:42:33 2005	OK - Access-Accept (1 attributes returned in 1.0s)
laurens.uninett.no	Thu Dec 8 09:42:33 2005	OK - Access-Accept (0 attributes returned in 1.0s)
radsec-toplevel.restena.lu	Thu Dec 8 09:42:33 2005	OK - Access-Accept (1 attributes returned in 0.0s)
radsec1.cesnet.cz	Thu Dec 8 09:42:33 2005	OK - Access-Accept (1 attributes returned in 1.0s)
radsec1.eduroam.acad.bg	Thu Dec 8 09:42:33 2005	OK - Access-Accept (0 attributes returned in 0.0s)
radsec1.eduroam.cz	Thu Dec 8 09:42:33 2005	OK - Access-Accept (1 attributes returned in 1.0s)
showcase.surfnet.nl	Thu Dec 8 09:39:35 2005	OK - Access-Accept (4 attributes returned in 0.0s)
surplus.surfnet.nl	Thu Dec 8 09:39:35 2005	OK - Access-Accept (0 attributes returned in 0.0s)
tomasek.cz	Thu Dec 8 09:39:35 2005	OK - Access-Accept (1 attributes returned in 0.0s)