Ассоциация RENAM

MD-GRID CA:
планы и пути развития

Алексей Алтухов
alexx@renam.md

RENAM
Молдова

www.renam.md

MD-GRID CA – пути развития

- Создание нового центра сертификации (CA) для удовлетворения нужд научно-образовательного сообщества.

- Разработка и ввод в эксплуатацию сервиса eduRoam – сервиса для упрощения аутентификации и авторизации мобильных пользователей и их доступа к сети интранет/интернет

Определение Центра сертификации

- **Центр сертификации** или **Удостоверяющий центр** (англ. *Certification authority, CA*) — это организация или подразделение организации, которая выпускает сертификаты ключей электронной цифровой подписи, это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

MD-GRID CA – текущее состояние

- Центр сертификации MD-GRID CA существует и успешно функционирует с 2009 года.
- Аккредитован организацией EUGRID-PMA
- MD-GRID CA является аккредитованным членом EUGridPMA, политика этой организации допускает выдачу сертификатов научных организациям Молдовы

EUGridPMA

- EUGridPMA это организация Авторитетов сертификации (Certification Authorities – CA) европейской научной среды (грид). В её составе больше 30 европейских стран. Ей регулярно проводятся семинары, чтобы обсудить и проработать все тонкости сертификационной технологии, проводить взаимный аудит безопасности, а также выработать общую стратегию пользования цифровой подписью в европейской научной е-среде. В семинарах обсуждаются пути повышения уровня безопасности при использовании цифровых подписей, возможности их использования не только физическим лицом, но также компьютером (сервером) и программной авторизацией и аутентификацией.

- Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем самоподписанного сертификата в списке удостоверенных корневых сертификатов. Корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом, аккредитованный центр получает «техническое право» работы и наследует «доверие» от организации, выполнившей аккредитацию. Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией, проводящей аккредитацию в своих интересах и в соответствии со своими правилами

Новый Сертификационный Центр MD-GRID CA

Новый Сертификационный Центр открытых ключей будет отвечать за

- регистрацию пользователей
- предоставление пользователям научно образовательных учреждений Молдовы доступа к национальным, европейским и мировым ресурсам и хранилищам данных.

Использование сертификатов

Сертификаты пользователей могут быть использованы для:

- электронной подписи при электронной переписке и других видах электронного документооборота.
- аутентификации и авторизации пользователей с целью получения доступа к ресурсам и сервисам, предлагаемым Академией Наук Республики Молдова и научно-образовательной сетью RENAM
- доступа к ресурсам научно-образовательных сетей других стран, а также сервисов, разработанных в рамках проектов ЕС

Пути создания нового Центра сертификации

- Создать собственные CA, которые будут обслуживать потребности ассоциированных сервисов и установить отношения доверия между этими CA;

- Направить запросы сертификатов к общедоступным CA, предназначенным для обслуживания потребностей определенного региона или проекта. Сертификаты таких CA находятся в открытом доступе в соответствующих репозиториях. Примером такого репозиторию может выступать сайт http://www.eugridpma.org организации EUGridPMA. Этот репозиторий содержит сертификаты сертификационных центров, которые обслуживают потребности разнообразных проектов, которые реализовываются в Европе и других частях мира;

- Использовать комбинированный подход, при котором одни создаются отдельные собственные CA, а другие используют открытые CA, политика которых отвечает направлению деятельности или региона расположения этих сегментов.

В процессе создания и дальнейшей работе нового Центра Сертификации планируется использовать **комбинированный подход**.

Federated network access with

Where Ever You May Roam (C)

Slides courtesy of
Klaas Wierenga,SURFnet

Agenda

- What is **eduroam**?
- What does this mean?
- Where can I connect to eduroam?
- How do I get more information?

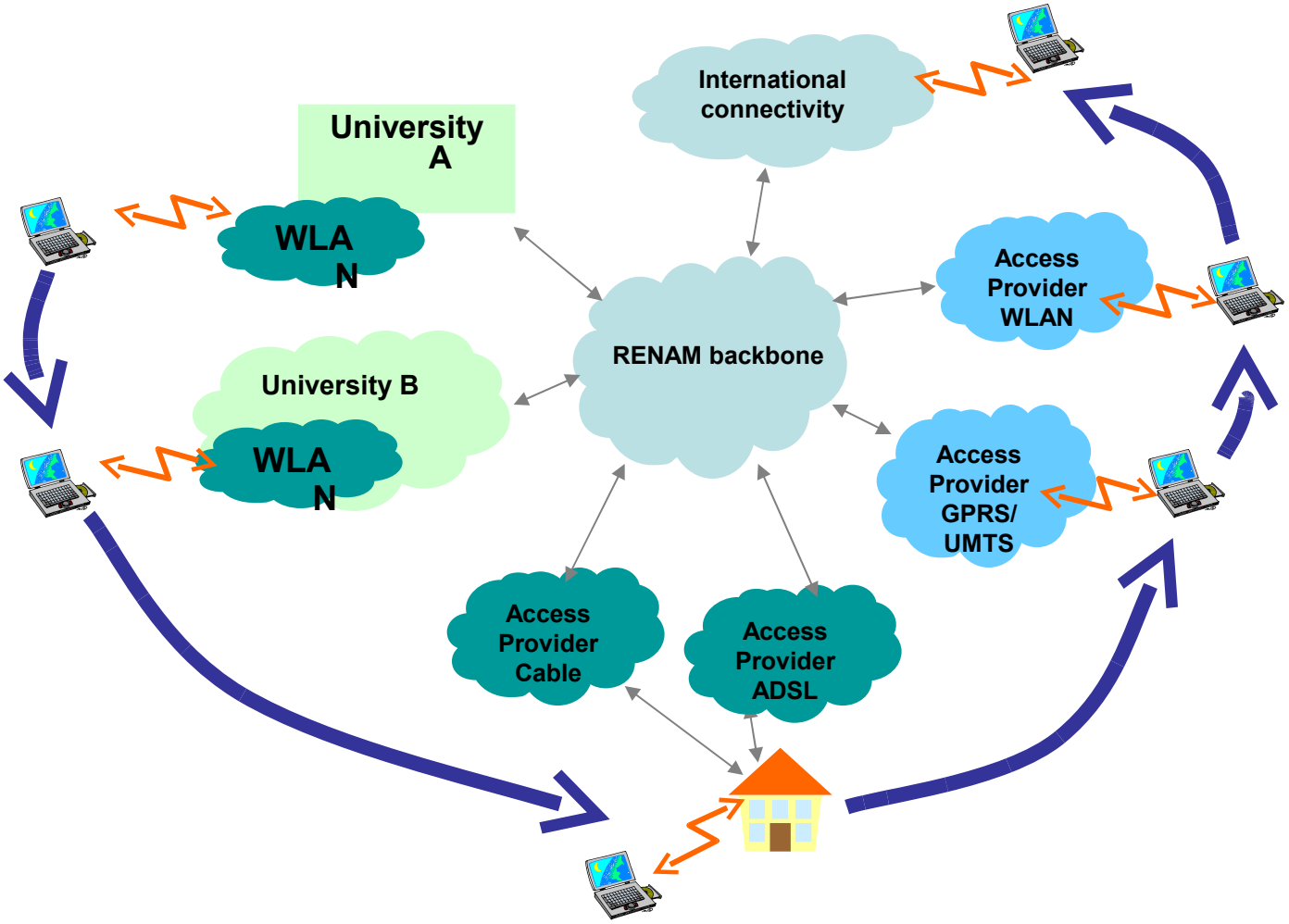
(European) eduroam service

- eduroam user experience: “open your laptop and be online”
- To provide secure network access inside the confederation boundaries (to the end users)
- eduroam is a secure international roaming service for members of the European eduroam confederation (a confederation of autonomous roaming services)
- **First steps in transition to service:**
  - **Service Definition and Implementation Plan**
  - **Policy**

What Is eduroam

- eduroam stands for Education Roaming
- RADIUS-based infrastructure
- Uses 802.1X to allow inter-institutional roaming
- Uses WPA/WPA2 encryption
- Allows users visiting other eduroam institutions to access WLAN using home credentials

Users are mobile



eduroam goes global

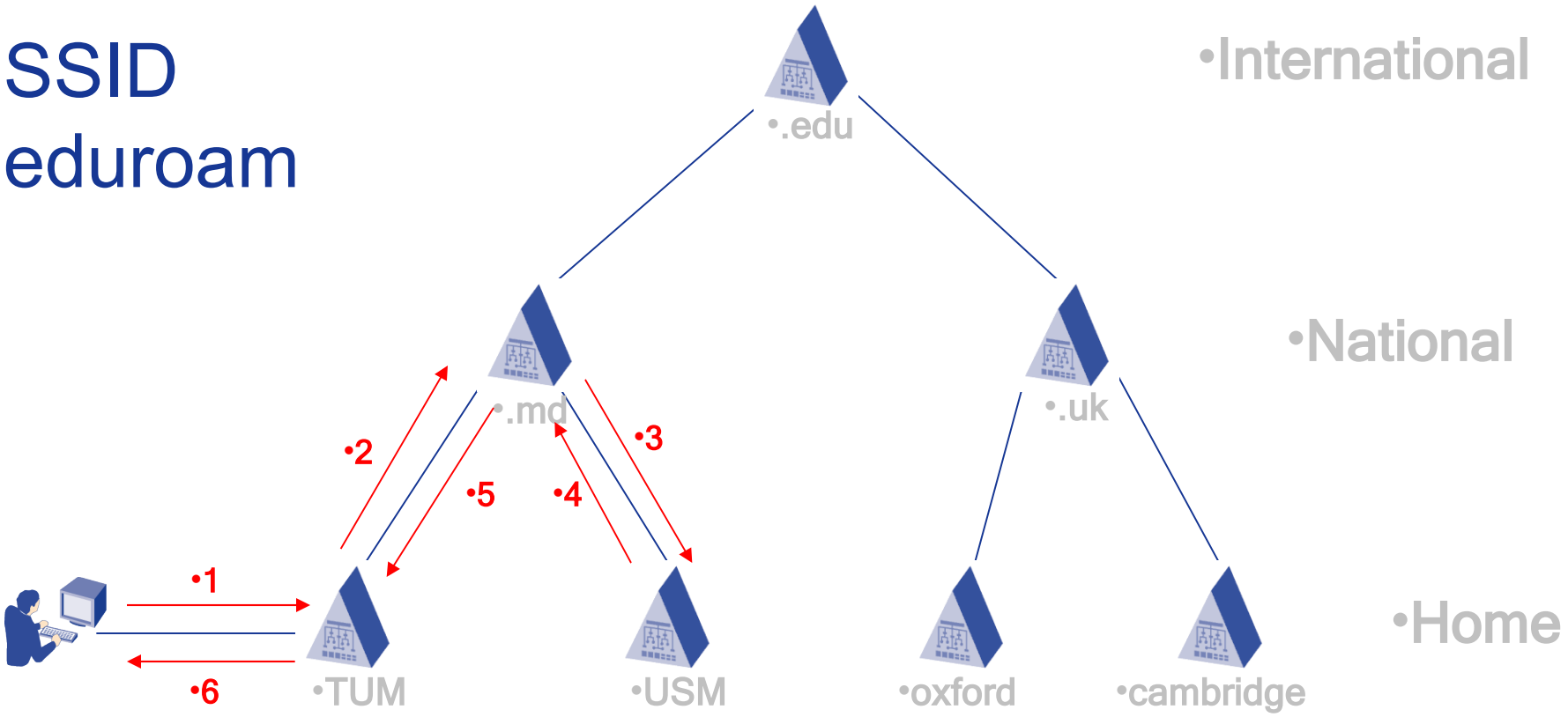
http://www.eduroam.org

What Does This Mean?

- The ability to access your resources at other institutions.
- No waiting for temporary accounts
- Don’t have to set up temporary accounts
- Same username and password when traveling.
- No down time in cross institutional meetings or research groups.
- Global roaming.
- Freedom

How it works!

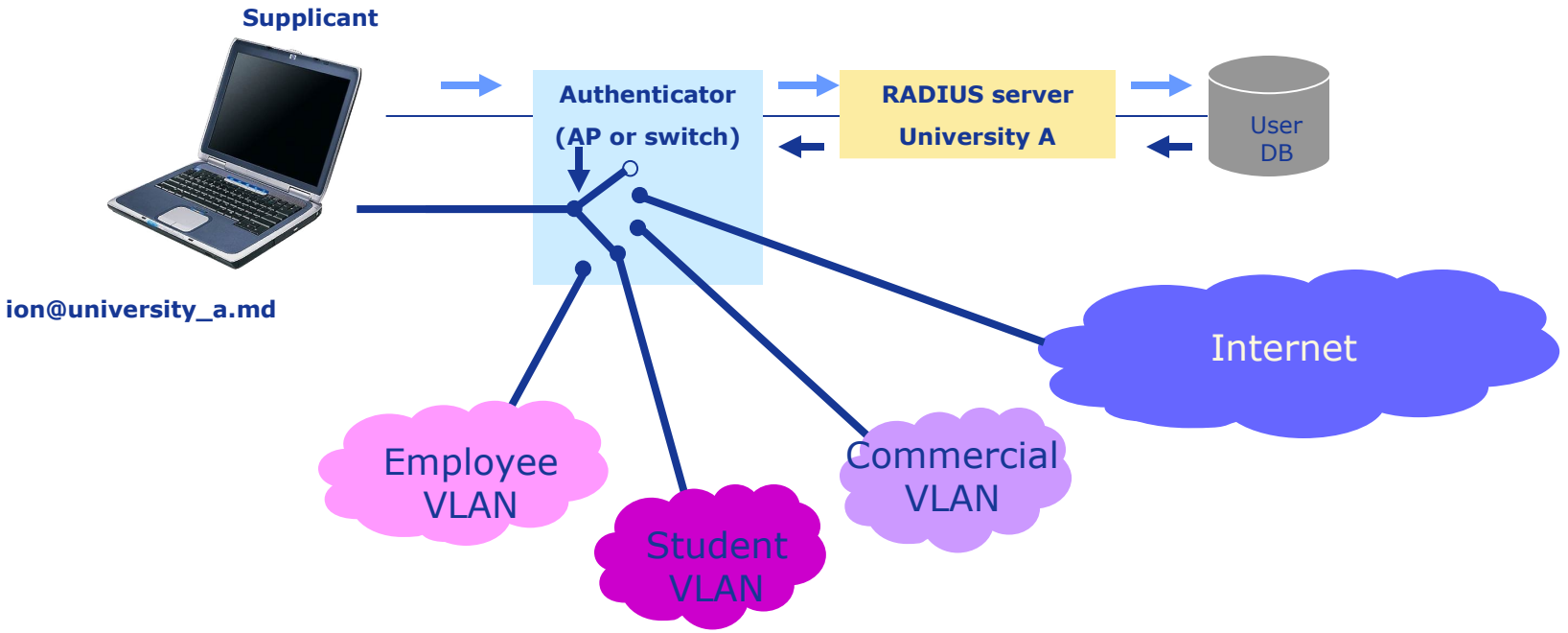
- SSID
  eduroam



eduroam architecture

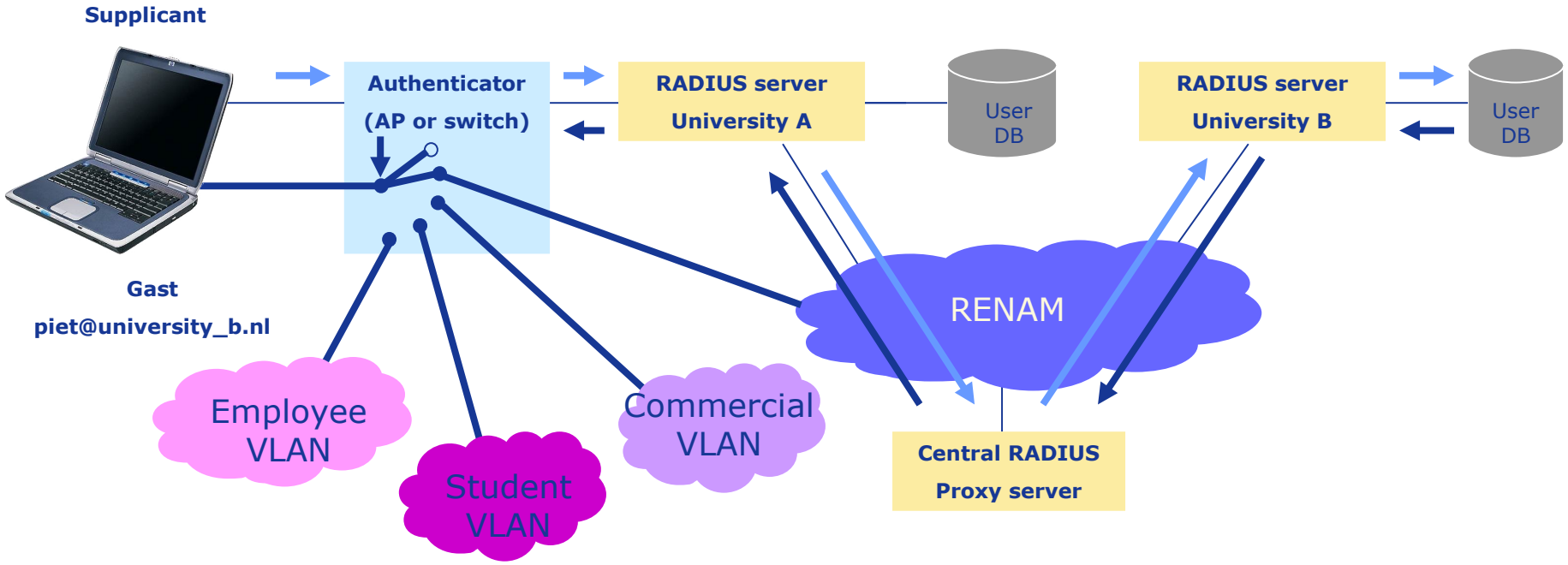
- Security based on 802.1X
  - Protection of credentials
  - Provides basis for new wireless security standards WPA and 802.11i
  - Different authentication mechanisms possible by using EAP (Extensible Authentication prototcol)
    - Username/password
    - X.509 certificates
    - SIM-cards
  - Integration with VLAN assignment
- Roaming based on RADIUS proxying
  - Remote Authentication Dial In User Service
  - Transport-protocol for authentication information
- Trust fabric based on:
  - Technical: RADIUS hierarchy
  - Policy: Documents/contracts that define the responsibilities of user, institution, NREN and the eduroam federation

Secure access to the network with 802.1X



- 802.1X
- (VLAN assigment)

eduRoam



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

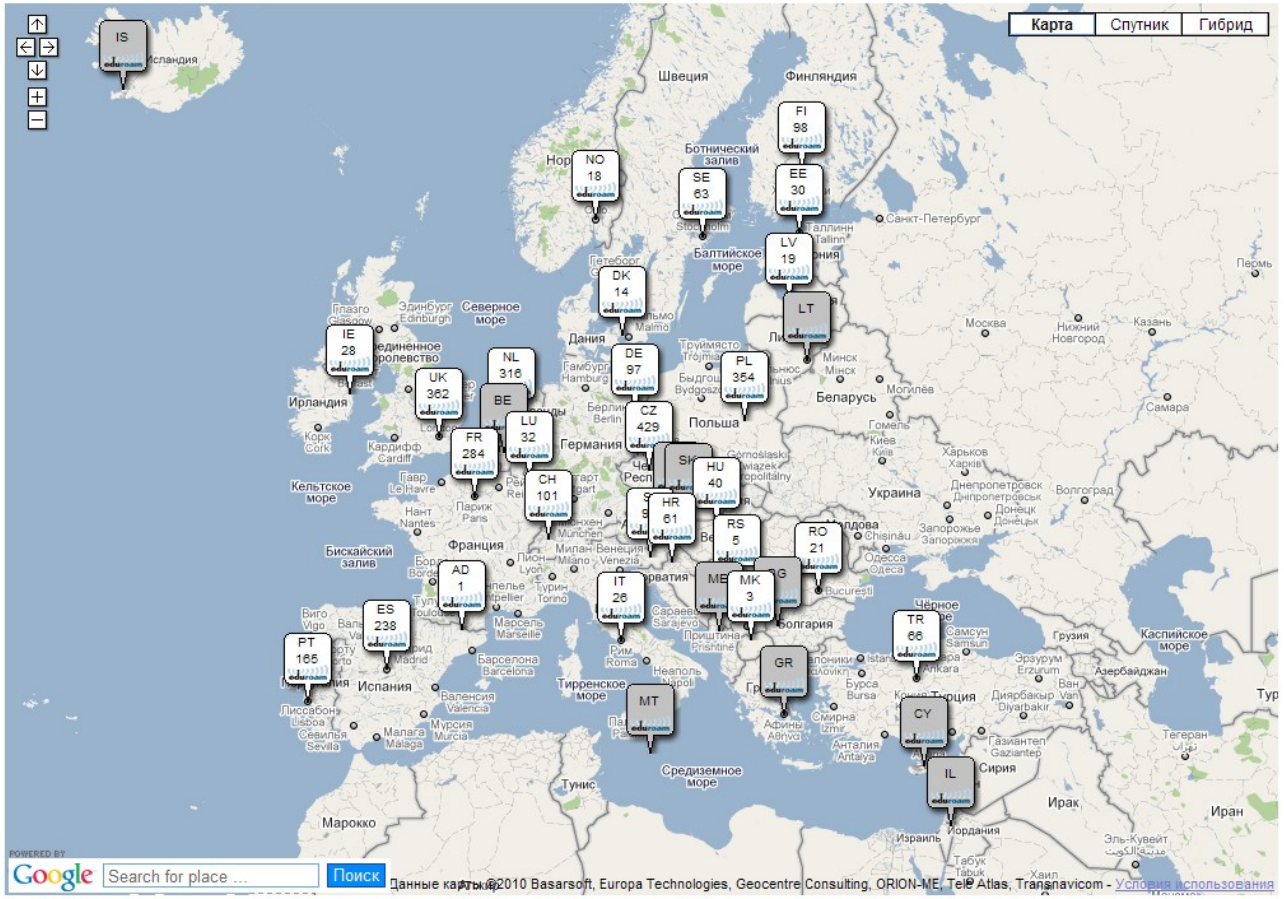
The European eduroam policy

- Mutual access
- Home institutions are/remain responsible for their users abroad
- Members are NRENs
- Members guarantee required security levels by their participants
- Members promote eduroam in their countries
- European eduroam may peer with other regions

National policy

- Mutual access
- Members are connected institutions
- Home institution is/remains responsible for its users behaviour.
- Home institution is responsible for proper user management
- Home and visited institution must keep sufficient logdata
- Appropriate security levels

Status of *eduroam*



- Over 500 institutions in Europe, Australia and Taiwan, Canada

- USA, Japan, Korea have followed shortly

eduroam coverage

Joining eduroam for an institution

- Set-up your local 802.1X infrastructure
  - Accept requests for your-domain.cc-tld and process them
  - Proxy requests for non-local users to the national server
- Send an (encrypted) e-mail to your NREN with:
  - FQDN of toplevel RADIUS-server(s)
  - IP-addresses of toplevel RADIUS-servers
  - Shared secret to use between your and their server(s).
  - URL of your eduroam website
  - Information about test-account
  - Contact details admin
- Sign the policy document

Conclusions

- 802.1X provides secure, scalable access to the campus network
- Enabling eduroam is a easy once 802.1X is in place
- Many have already joined, so

Join….

More information

- eduroam in SURFnet
  - http://www.eduroam.nl
- eduroam in Europe
  - http://www.eduroam.org
- TERENA TF-Mobility
  - http://www.terena.nl/mobility
- The unofficial IEEE802.11 security page
  - http://www.drizzle.com/~aboba/IEEE