Service mobilité eduroam.fr

Catherine Grenet (CNRS/UREC)

JoSy « mobilité »

Paris, 20 mars 2007

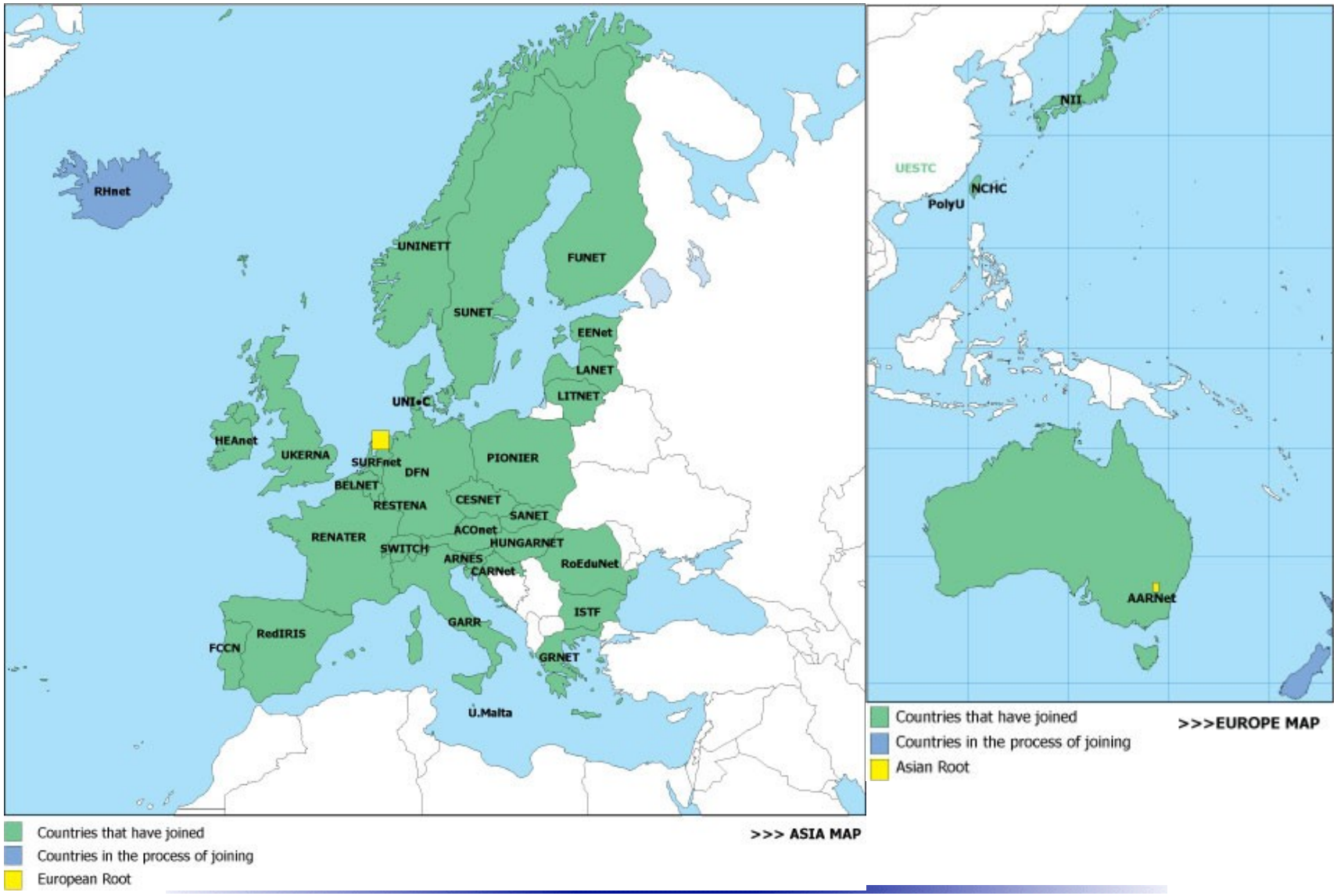
Plan

- Historique et objectifs
- Principe de fonctionnement
- Mise en œuvre
- Spécifications techniques
- Références

Historique et objectifs

- Initiative de la *Mobility Task Force* de TERENA (*Trans-European Research and Education Networking Association*) en 2003
- Fournir aux utilisateurs des réseaux education-recherche européens un accès à Internet lors de leurs déplacements d'un NREN à l'autre
- Principalement pour les accès sans fil
- Sécurité comparable à celle d'un accès filaire
- En réduisant au minimum la charge d'administration pour les établissements d'accueil
- Solution retenue : 802.1X + EAP : TLS, TTLS ou PEAP
- EduRoam → eduroam
- ARREDU → eduroam.fr

Couverture : Europe et Asie



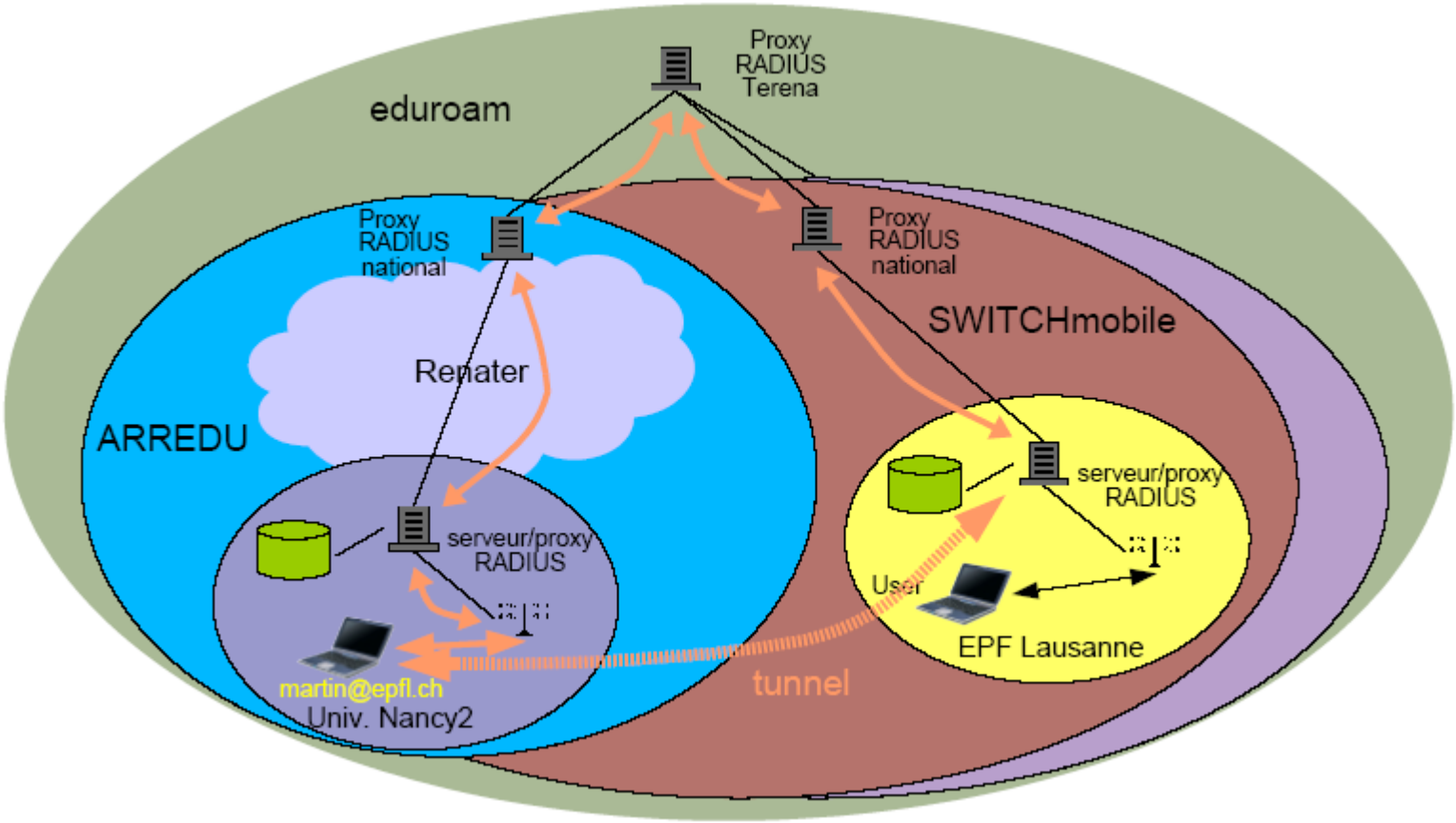
Couverture : France

- 33 établissements

Principe de fonctionnement

- L'utilisateur se connecte avec le(s) même(s) identifiant / mot de passe / certificat que sur son site d'origine
- Système d'authentification réparti reposant sur une hiérarchie de serveurs RADIUS
- Le serveur racine est géré par TERENA (Amsterdam)
- Le serveur national eduroam.fr est géré par le CRU, il est doublé par un second serveur hébergé au CRC (Strasbourg)

Principe de fonctionnement



Mise en œuvre

- Demande de modification de l'agrément Renater (via SAGA)
  - Désignation du correspondant eduroam
  - Intégration de la charte eduroam.fr à l'agrément
  - Renater est garant auprès de TERENA
- Création du compte eduroam.fr
  - Géré par le CRU
  - Permet de gérer les informations associées au service :
    - Nom(s) de domaine
    - Adresses, ports, secrets partagés des serveurs RADIUS
    - Autres informations...

Charte eduroam.fr

- La charte eduroam.fr engage à :
  - Mettre en œuvre un service d'authentification conforme aux spécifications techniques
  - En tant qu'établissement de rattachement :
    - Informer ses utilisateurs : existence du service, manière d'y accéder, respect des règles d'utilisation des réseaux visités
    - Offrir une assistance technique à ses utilisateurs
  - En tant qu'établissement visité :
    - Mettre en œuvre le service au travers de points d'accès sans fil
    - Informer les visiteurs sur l'existence du service et ses conditions d'utilisation
  - Sécurité du service :
    - Chiffrement de bout en bout des données d'authentification
    - Chiffrement efficace sur les points d'accès sans fil
    - Sécurité des serveurs RADIUS
    - Traces : pouvoir identifier l'utilisateur d'une adresse IP à un moment donné

Spécification techniques

- Nom de domaine (*realm* RADIUS) : en principe un domaine DNS, doit se terminer en .fr
- Radio : 802.11b / g, canaux 1 à 11
- SSID : « eduroam », diffusé si possible
- Authentification : 802.1X + EAP-TLS, TTLS ou PEAP (à l'exclusion de tout autre)
- Chiffrement du lien radio : AES ou TKIP, à défaut WEP dynamique (128 bits avec changement de clé toutes les 2 mn)
- Fourniture d'un service DHCP aux clients
- Protection du réseau d'accueil vis-à-vis de l'extérieur

Spécifications techniques

- Services réseau accessibles
  - Il ne devrait pas y avoir de filtrage en sortie
  - A défaut, les services suivants doivent être autorisés :
    - HTTP, HTTPS
    - DNS
    - ICMP (echo request, echo reply)
    - IPsec (ESP, AH, IKE)
    - OpenVPN
    - ssh
    - POPs, IMAPs
    - NTP
    - SMTP sur le serveur de messagerie local

Références

- Site de référence : http://www.eduroam.fr/
- Présentations Tuto JRES 3 : http://www.jres.org/tuto/tuto3.php
- Liste de diffusion : http://listes.cru.fr/sympa/info/eduroam.fr