

# Terena Networking Conference 2003

---

## Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET)

Sami Keski-Kasari <samikk@cs.tut.fi>  
Karri Huhtanen <karrih@cs.tut.fi>

# Contents

---

- 1. Background
    - 1.1 What is Public Access Roaming?
    - 1.2 Why Public Access Roaming?
  - 2. Architecture
    - 2.1 Network Architecture
    - 2.2 Roaming Architecture
  - 3. Current State of Public Access Roaming
  - 4. Requirements for Organizations
  - 5. Security Issues
  - 6. Links and Contact Information
-

# 1.1 What is Public Access Roaming?

---

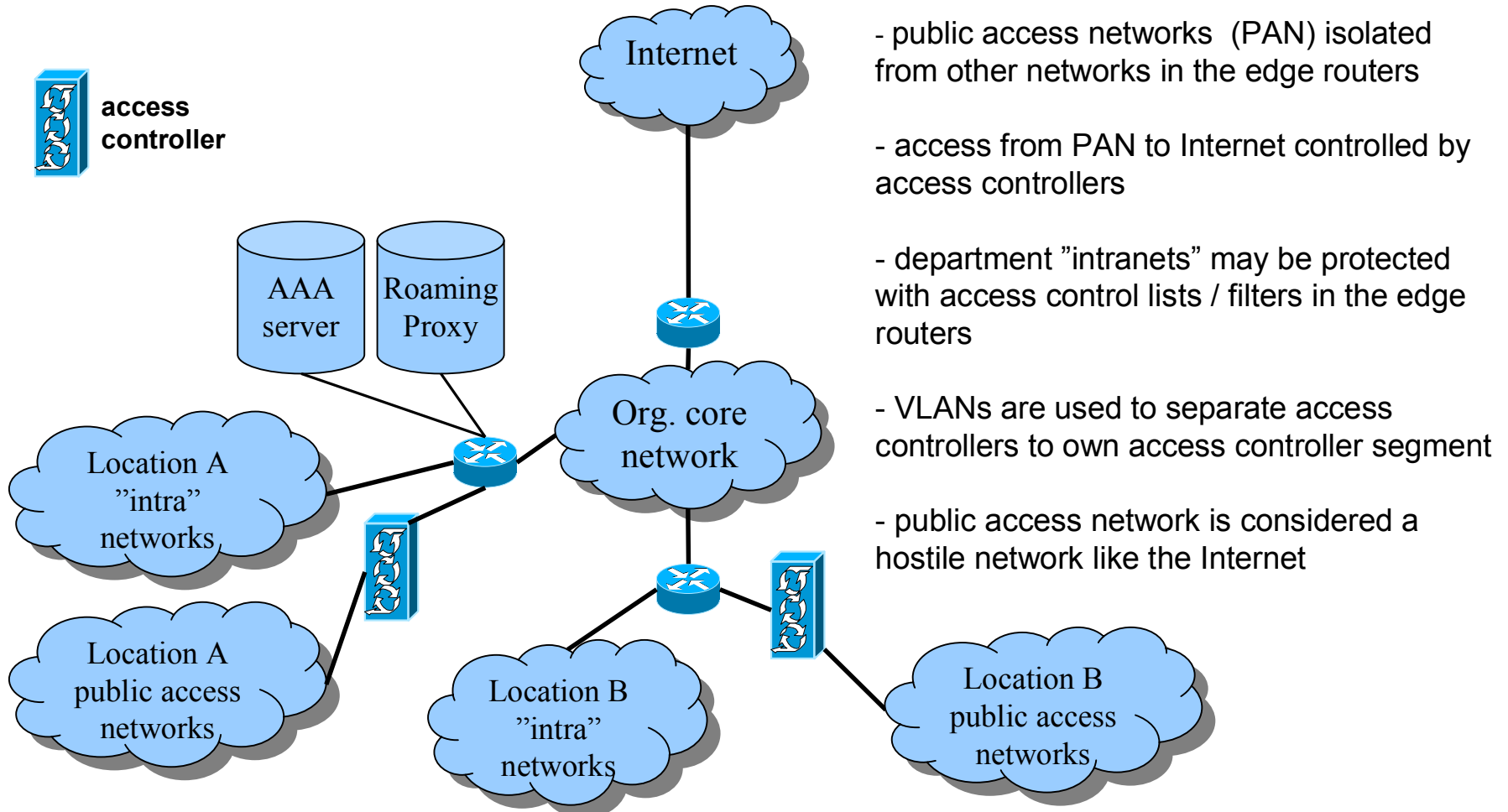
- Public Access is an authenticated temporal access to the network via both wireless or wired medium.
- Public Access Roaming is a way to transfer authentication information between organizations so that an user from different organization may gain public access to organization's network she's visiting.

## 1.2 Why Public Access Roaming?

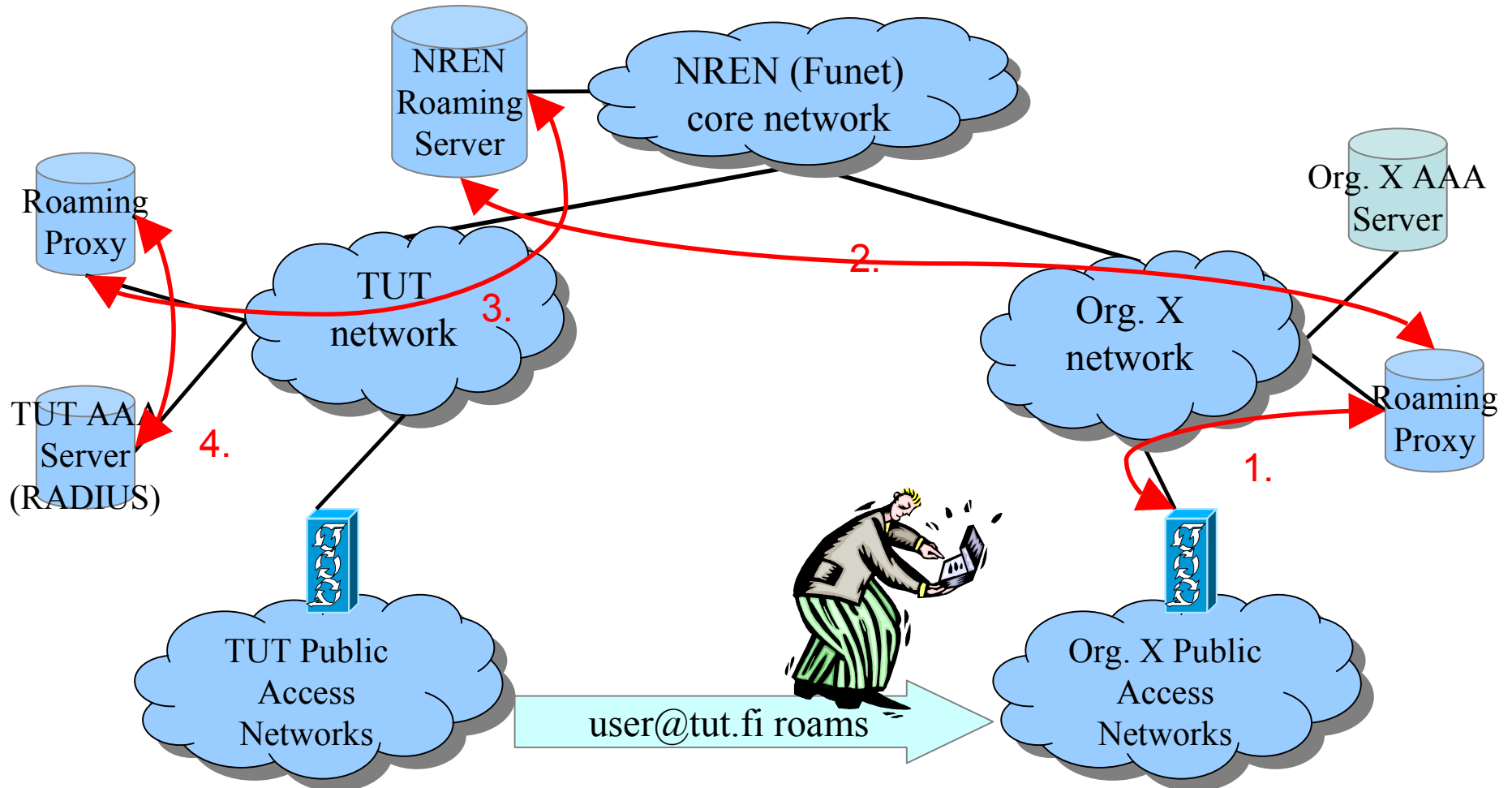
---

- The mobility of the students, faculty members, project personnel, visiting lecturers etc. between organizations is constantly increasing.
- The existing network access authentication schemes are different between organizations and even inside one.
- The authentication databases are separate and each organization is its own island without mutually agreed way to transfer authentication information between others.
- The usability of the public network access is poor:
  - different authentication methods and network environments confuse the end user
  - every visiting user may require extra support from the system administration to be able to gain the network access

## 2.1 Network Architecture



## 2.2 Roaming Architecture



## 3. Current State of Public Access Roaming

---

- In Tampere region Tampere University and Tampere University of Technology have both a network architecture capable of public access roaming.
- In Vaasa region the local Funet organizations are building public access network infrastructure that is interoperable with Tampere universities' network infrastructure.
- Regional roaming comes first defining policies and practices and inter-region roaming follows.
- After inter-region roaming comes inter-NREN-roaming currently under work in Terena's Mobility Taskforce

## 4. Requirements for Organizations

---

- User account database (username, password), preferably with Radius interface, but also LDAP/Diameter is/will be possible
  - Free or commercial public access controller(s), that can do TLS/SSL-secured webpage-based authentication using Radius-servers (e.g. Oasis, NoCatAuth, Nokia, Nomadix, Vernier Networks)
  - Certificate Authority to generate the certificates needed for access controllers
  - An UNIX/Linux/\*BSD host for Public Access Roaming Proxy functionality, if converting the existing AAA server is not viable
  - Open mind, desire to work together, the support of the system administration staff
-



## 5. Security Issues 1/2

---

- Server / Network element security
  - Badly maintained Access Controllers, Roaming Proxies, AAA servers
  - Depending of host's location in the network, compromising it may jeopardize all user accounts of the roaming organizations.
  - Allowing only IPSEC-secured traffic between network elements is not THE Solution as systems may be compromised locally via other network daemons like SSH and SNMP.
- Certificates and distribution
  - The handling of network element certificates becomes more important as we cannot expect the end user to install several self-signed CA certificates into her terminal => soon we have need for a common PKI infrastructure handling trust relationships between organizations and NRENs.

## 5. Security Issues 2/2

---

- Security policies and legal issues
    - Is it allowed to transfer username-password –pair between organizations and what are the conditions for that?
    - What about the statistics gathered from the users (traffic amounts / profiles)? In what detail they can be stored, researched or followed?
  - Trust issues, roaming policies and practices
    - For organizations to be able to trust each other and to roaming partners' capability of securing and maintaining their systems, the roaming organizations must together define the roaming architecture and policies based on practical issues.
    - This may not be very far from roaming/peering agreements between cellular and Internet operators.
-

## 6. Links and Contact Information

---

- Network Architecture:
  - TUT Public Access Architecture:  
<http://www.atm.tut.fi/tut-public-access/>
- Roaming Architecture:
  - <http://www.atm.tut.fi/public-access-roaming/>
- Contact Information:
  - Sami Keski-Kasari <[samikk@cs.tut.fi](mailto:samikk@cs.tut.fi)>, Public Access Roaming
  - Karri Huhtanen <[karrih@cs.tut.fi](mailto:karrih@cs.tut.fi)>, TUT Public Access Architecture