
## Mobility Task Force

## Deliverable C

# Requirements definitions for inter-NREN roaming

### Version 1.4

**Authors:** Jürgen Rauschenbach, Carsten Bormann, Niels Pollem;

**Contributions:** all

## Abstract

Wireless LAN technology (WLAN, according to IEEE 802.11*) is already an important part of the infrastructure at universities and research institutions connected to the NRENs in Europe. Based on local experience the TF will try to identify requirements on an inter-NREN roaming architecture, filter out recommendations and propose solutions to make secure wireless LAN access from different locations with different authentication systems more transparent to the user. This deliverable will list the requirements currently known to reach this goal.

This is a document of the TERENA TF „Mobility“.
See Terms of Reference on http://www.terena.nl/tech/task-forces/tf-mobility.
The table of planned deliverables can be found here:
http://www.terena.nl/tech/task-forces/tf-mobility/docs/DelList.pdf

# 1. Introduction

In preliminary meetings various NRENs (including DFN, SURFnet, SWITCH and UNINETT) reported about activities going on in their countries to introduce and use WLAN technologies. Concepts for a Notebook University are under development including the introduction of wireless network devices into the learning and teaching processes. The number of institutions with WLANs is growing and the number of users in every institution is increasing too. It is going to be common to have access to the network from almost every building or via wireless connectivity across the campus. If possible this wireless connectivity will be extended to the public areas such as towns and city areas so that students may access the university network independent of their physical location using WLAN technology. This all makes it necessary to implement security measures to avoid abuse by unauthorised users.

The measures taken by academic institutions differ significantly, sometimes even between different departments of the same institution. Because of this, there can be incompatibility and scalability issues at the institutional level, let alone at the national level or beyond. These problems have encouraged NRENs to look at developing a more generalised approach to solve these problems and work towards the creation of an architecture for “roaming” between WLANs, in particular between organisations on a national or European level, to support the travelling scientist/teacher in a nomadic computing scenario.

# 2. Terminology

There are two glossaries of terms, together forming the TF’s deliverable B: technical definitions and the non-technical terms that are used to describe current and proposed solutions. See deliverable B for details.

# 3. Requirements Definitions

The objective of the taskforce effort is to enable NREN users to gain wired or wireless network access either to the Internet or their home institution network (via the NREN or Internet) while visiting in another NRENs’ member institutions in Europe. As this requirement is related to solutions on the national level the results of the project are of value for the NRENs own roaming solutions, too.

When a user connects to a WLAN anywhere in the community of the NRENs the following requirements for the roaming solution should be met as closely as possible:

### *Major requirements:*

- The **scalability** of the proposed solution must be maintained and the **administrative overhead** must be minimised.
- The required **security** must be maintained for all partners in the process.

### *Minor requirements:*

- The **usability** must be good for all needed/used platforms.
- An **accountability and logging functionality** must be provided to track abuse.

Where not possible a reasonable trade-off should be found.

These requirements are described in more detail in the following sections.

## *3.1. Scalability and Administrative Overhead*

The decision about local administration procedures is surely out of the scope of the TF. However it could be helpful to provide recommendations to make clear what kind of

procedures are helpful for roaming solutions and what kind of procedures could make this harder. In any case, the technical architecture must not have any characteristics that make it impossible to attain the goals described below.

The first goal is to **minimize the administrative extra effort** for roaming per user. A small amount of administrative overhead may be acceptable at the home institution, in order to prepare any specific user for European roaming. However, any extra administrative effort that occurs at the visited institution per roaming occurrence is unacceptable – the chilling effect on inter-NREN roaming would be too great.

As far as possible, roaming users must be accommodated using the existing infrastructure. E.g., it is unacceptable to require adding access control devices to each site for the sole purpose of enabling roaming. If any additional systems are required, their complexity should be minimized. The existing authentication and authorisation procedures (AAA) at the home institution (nowadays, often based on the protocol RADIUS) must work as smoothly as possible with the additionally systems required. The **scaling** properties must allow use on a European level (e.g., any $n^2$ work is unacceptable).

Any regulatory or legal entanglement must be avoided. E.g., administrative procedures should be examined with respect to data protection laws and with respect to telecommunications regulation. (However, note that complete protection of user location information is unattainable at the moment; see 3.2 below.)

### *3.2. Security Requirements*

The obvious **security requirement** is that the roaming access must only be available to authorized users, which should include all users authorized for Internet access at the NREN member institutions participating in the roaming scheme. The visited institution may want to have more fine-grain control about this authorization, e.g. in order to control troublemakers while causing the least disruption to other roaming users. In any case, the scheme must provide accountability for each individual user (even if the identity of that individual user may be opaque to the visited institution, this may be provided by chaining back to the authorizing institution).

Users expect a certain level of privacy against casual snoopers when using the wired Internet. While it can be argued whether this expectation is wise, a nice-to-have would be to maintain about the same level of privacy in a visited network, as well as some protection against data manipulation and session hijacking. Obviously, some access control solutions in use today cannot provide this level of security.

Whatever the security properties of the roaming scheme in use are, it must not impede the use of additional security measures by the roaming users (visitors), such as IPSec and VPN technologies. It is well-known that NAT (and, in particular, port-translating NAT) solutions cause problems with these protocols.

Finally, the roaming solution should not aggravate existing security issues of the visited networks.

Two non-goals are notable in the security area:

- In contrast to cellular networks, there is little need to “protect” the WLAN – the ISM spectrum in use cannot be protected in any case. This argument does not extend to the fixed network connecting the access points, but in many cases this has a much higher bandwidth than the WLAN itself.
- With current technology, it is very hard to reliably conceal the approximate position of the user, at least to participating network elements in the user’s home network. Location privacy will only be attempted where it is easy to attain.

### *3.3. Usability Requirements*

The roaming solution must be available to most current users of WLANs at NREN member institutions, preferably also to existing users of wired networks. This means it should be standards based (no proprietary solutions) and zero- or at least low-cost. Preferably no installation of new software should be required at the client just to enable roaming (alternatively, additional software must be useful for local use and must be easy to obtain and available for most client platforms in use today, including Windows versions of the last 5 years as well as Mac OS X and Linux). Different devices like PDAs and others should be supported.

The proposed solution must not be overly complex, thus causing excessive overhead reducing user bandwidth/throughput rates. Still, roaming users need to be aware that they might neither experience the throughput rates of wired networks nor that of their local wireless network.

While current deployments still focus on IPv4, IPv6 must be incorporated in the European-level architecture.

For many applications, it is useful to be able to directly access home institutions and to obtain an IP address in the home network; this could be part of the roaming architecture or supported using additional protocols such as Mobile IP or VPN-style tunnelling protocols.

It is also useful to enable guest access to resources within the visited site, such as printers, presentation devices etc. To enable local work in the visited institution, methods such as Service Location Protocol (SLP) should be investigated. Obviously, the authorization issues involved will be multi-level and therefore more complicated than for simple Internet access (e.g., rights for specific users, user classes etc.).

### *3.4. Accounting and Logging*

Whilst the security features installed should make it difficult to abuse the services provided to guests in a network, this can not be ruled out. To ensure that the institution is not unduly tarnished in any way by the actions of visitors using its network or by its local users using other institutions networks, it is required that the proposed solutions include an easy to deploy user accountability system. It should be feasible to extract necessary data from this system to analyse what happened in case of misbehaviour and to track any abuse. As national data protection laws are different it is difficult to judge whether this requirement can be fully met at this project stage.

It is difficult to define a “violation”, because the rules therefor are not standardised; e.g. in the DFN environment the universities are usually defining their own AUP (Acceptable Use Policy). It may be desirable to create a catalogue of “events” that should be tracked. In any case deemed serious, the CERT (or similar organisation) of the affected NRENs should be contacted.

## 4. Regulation/Legislation issues

There are two levels of regulation/legislation: the national level and the European level. Both are relevant to the TF. An overview of these regulations should be compiled for reference. The proposed solutions should avoid any violations, especially of the participating countries’ data protection laws.