

24.05.05

# Deliverable DJ5.1.2: Documentation on GÉANT2 Roaming Requirements

## Deliverable DJ5.1.2

Contractual Date: 28/02/2005  
Actual Date: 24/05/05  
Contract Number: 511082  
Instrument type: Integrated Infrastructure Initiative (I3)  
Activity: JRA5  
Work Item: 2 (Roaming)  
Nature of Deliverable: R (Report)  
Dissemination Level: PU (Public)  
Lead Partner: SURFnet  
Document Code: GN2-05-071v6

**Authors:** J. Rauschenbach (DFN), K. Wierenga (SURFnet): main editors; contributions from D. Lopez (RedIRIS), M. Milinovic (CARNet/SRCE), S. Papageorgiou (GRnet), R. Papez (ARNES), J. Sankar (UKERNA), D. Simonsen (NORDUnet/UNI-C), S. Winter (RESTENA),

## Abstract

The objective of this deliverable is to identify and to classify the requirements of the federated GÉANT2 Roaming Infrastructure that GÉANT2 JRA5 is going to build to provide location-independent access to networks.

Project:	GÉANT2
Deliverable Number:	DJ5.1.2
Date of Issue:	24/05/05
EC Contract No.:	511082
Document Code:	GN2-05-071v6

# Table of Contents

0	Executive Summary	iv
1	Introduction	1
2	Scenarios for Roaming	4
2.1	The general AAI Problem	4
2.2	The Network Access Scenario	5
3	General Requirements	8
3.1	Security Requirements	8
3.2	Standards Compliance and Integration	9
3.3	Operational Requirements	9
4	Requirements on selected Building Blocks	11
4.1	Federation Service	12
4.2	Local Federation Connector	12
4.3	Identity Management	13
4.4	Federation Documents	13
4.5	Authentication and Authorisation Mechanisms	13
5	Conclusions	15

## Table of Figures

Figure 2-1: Federation Service as trust fabric between the home and remote AAI	5
Figure 2-2: Communication pattern during network access control.	7

## 0 Executive Summary

The objective of GÉANT2 JRA5 is to develop a pilot service infrastructure for authentication and authorisation for the education and research community in Europe, supporting multiple domains and variable authentication and authorisation systems. The two work items JRA5 is dealing with in the first project year are Roaming and AAI. The GÉANT2 AAI shall support seamless and location-independent access to applications, services and other resources and provide authentication and authorisation services to other GÉANT2 activities. These requirements are outlined in the deliverable DJ5.2.1 (AAI requirements document). The current document (DJ5.1.2) is focussed on Roaming requirements. It preserves the same structure, same basic model and the same terminology (see also DJ5.1.1 “Glossary of Terms”). This is done intentionally as both work items AAI and Roaming shall grow together into a single sign-on (SSO) solution.

Before a user can access any network-based service, he needs to get access to the network itself. The vision of JRA5 is to grant network access at any location and at any time in the federation, providing nearly equivalent conditions for the network access as in his home institution. The word roaming was originally used for providing connectivity to cellular phones not being connected to the home network. We are following the same basic idea, but the technology is different. The JRA5 goal is to create a federation of autonomous roaming infrastructures based on open standards, where the trust level is indicated by the requirements on each member of the federation.

The deliverable includes the description of a generic AAI scenario that illustrates the model of a federated AAI. The purpose of the federation is to act as a superstructure that makes inter-organisational authentication and authorisation possible. Roaming is seen as a special case of the generic model. The detailed sequence of steps in the authentication and authorisation process is presented for network access. The pilot roaming authentication service "EduRoam" ([www.eduroam.org](http://www.eduroam.org)) is a first real-life example of a federated AAI.

The general requirements on the roaming infrastructure are described from a generic and conceptual viewpoint. The level of conformance to these requirements will be a useful indication of how successful JRA5 is in the delivery of appropriate solutions. It is also worth noting that some of the requirements identified so far are inherently conflicting with each other. The “ease of use” requirement may conflict with the “reasonable security” requirement as an example. As a result, compromises may be inevitable in some cases. JRA5 has categorised the general requirements into three major groups as (1) Security, (2) Integration and standard compliance, and (3) Operation. Each group contains a set of requirements (major requirements are listed first). The more specific requirements in the document are related to known functional building blocks of a roaming infrastructure. They will prove to be a useful reference to determine AAI characteristics to support access to services as a necessary step towards SSO.

Project:	GÉANT2
Deliverable Number:	DJ5.1.2
Date of Issue:	24/05/05
EC Contract No.:	511082
Document Code:	GN2-05-071v6

# 1 Introduction

The growing share of mobile devices and technologies used in the daily work process of users in the NREN environments raises the request for support of the location independent access to resources and applications. The general scenario is that a researcher, when travelling with a WLAN enabled notebook or other mobile devices, wants to get transparent and secure network access at the visited institution. The idea is now to span a mobility solution across Europe (and beyond) for researchers and scientists, travelling or temporarily staying at other locations, that enables them to work from those places with very similar conditions as they are used to at their home institution. In JRA5 this is called roaming and the enabling infrastructure is the roaming infrastructure.

The roaming infrastructure that GÉANT2 JRA5 is going to build will enable seamless sharing of network resources. There are two basic problems to solve: the technical provisioning and the trust establishment between the partners. While the technical part is not too complicated, the federation part needs work on policy development and trust building agreements. The goal is to apply a set of harmonised AA practices within the GÉANT2/NREN environment. The solution shall be based on open standards. In order to minimise the cost of user and privilege administration (e.g. access rights) and to provide a distributed and scalable solution, the chosen design shall facilitate federated Identity Management and inter-domain authentication.

Especially in roaming, JRA5 developments do not start from the ground up. They have to take into account that location-independent network access was already established by a number of NRENs and universities, e.g. in the EduRoam project ([www.eduroam.org](http://www.eduroam.org)). Therefore it is fundamental to be able to integrate existing national and local systems by grouping existing components based on reasonable trust levels and to provide a federation service between them. In order to build a federated roaming solution, interfaces to ensure a smooth interoperability must be defined and service elements must be created.

The GÉANT2 roaming infrastructure shall be downward compatible to EduRoam and preserve the functionality and policy results available so far. There will however be improvements to the current solution, both technically and organisationally.

The combination of the underlying technologies for EduRoam, viz. the IEEE 802.1X standard on the client and a hierarchy of RADIUS servers, was first piloted in a research project carried out by SURFnet and taken up by TERENA's task force TF-Mobility as one of the most promising solutions. Extended with other popular access technologies (web-redirect with RADIUS infrastructure and VPN support) this resulted in the EduRoam pilot and its further rollout.

Project:	GÉANT2
Deliverable Number:	DJ5.1.2
Date of Issue:	24/05/05
EC Contract No.:	511082
Document Code:	GN2-05-071v6

The first experiences with EduRoam have shown the need for research into a number of issues in order to achieve the goal of a scalable, robust and secure roaming infrastructure for academic Europe. This is what the work on roaming within JRA5 is going to deliver. To preserve the already achieved wide visibility of the EduRoam project the GÉANT2 roaming infrastructure will be called EduRoam-ng (EduRoam-next generation).

The difference between EduRoam and EduRoam-ng will be outlined in the roaming infrastructure architecture document, based on the analysis of the current pilot. However, we want to provide an overview about the fields of improvement, that we are focused on at this stage of the project:

- RADIUS hierarchy: In the current architecture a static trust fabric based on hop by hop RADIUS secrets exists, for the new architecture means of establishing more dynamic trust relations (i.e. DIAMETER, DNSsec etc.) will be explored.
- Federation: The federation in EduRoam is weak. It should be based on a stronger and formal documented platform.
- Policy: Policy and legal issues will be studied as an underlying basis for the federated trust fabric.
- Access technology: 802.1X is considered as being secure, new standards like 802.11i and WPA/WPA2 should be integrated seamlessly.
- User authentication: Web re-direct in the current form is not secure. This should be solved or its usage cannot be recommended. End-to-end (client to home institution) encryption of credentials will be required.
- Growth: The infrastructure shall increase in the number of countries participating and in the number of institutions in a membership country.
- Monitoring: Monitoring, tracking and tracing technologies will provide solutions for a more scalable, robust and secure roaming infrastructure than EduRoam can offer today.

One objective specific to the overall long-term goal of JRA5 is the following:

- Integration with AAI

The results of JRA5 are expected to be implemented in an operational environment provided by campuses, NRENs and international organisations like TERENA and DANTE. Whether this operational service will be an extension or a replacement of the current EduRoam pilot service remains to be seen.

A number of JRA5 NRENs have been amongst the initial users of the existing EduRoam infrastructure and among the recently joined ones. All necessary preparations will however be made to facilitate easy adoption by those NRENs, with their academic communities, that are presently not participating in JRA5 and thus extend the user community further. First non-European partners joined EduRoam recently, and world-wide co-ordination becomes desirable and is under preparation. A global co-ordination working group was established with participants from Europe, USA, Australia and Japan so far. The extension to Australia and the United States is mainly driven by the TF-Mobility and supported by GÉANT2 JRA5.

In accordance with the JRA5 project plan, the EduRoam-ng shall initially be oriented towards network access and will then be further extended to include access to applications and services as a first step towards single sign-on (SSO) solutions, in line with the AAI architecture. Network access and web services are of particular interest for this integration process. One of the necessary requirements to develop SSO is the ability to communicate assertions based on digital identity attributes.

This document describes the requirements for EduRoam-ng. Chapter 2 contains a standard usage scenario, and a scenario for the network access including the AA related interactions. Chapter 3 introduces the general requirements for the infrastructure defined by JRA5, enumerating and analysing the criteria that the EduRoam-ng shall meet in order to satisfy the needs for its intended use. Chapter 4 describes functional requirements, discussing first structural characteristics of the infrastructure, but not yet the architecture itself, to which a dedicated document will be provided later.

## 2 Scenarios for Roaming

The purpose of this chapter is to illustrate the requirements on the EduRoam-ng, thus providing a network access scenario with detailed steps. The general AAI model is used as the framework adopted to roaming.

### 2.1 The general AAI Problem

The general problem that has to be solved for EduRoam-ng, is the support of multiple domains and variable authentication and authorisation systems. While defining a network as a resource, the model provided in DJ5.2.1 still holds, i.e. the requirement is to provide a solution where a user U from a Home Institution HI wants to access or operate on a resource R in the Resource Institution RI, which owns the resource R (normally another NREN or institution belonging to the same federation, maybe in a different domain). An AAI federation superstructure is needed, that knows where to send and receive requests across multiple federations and domains. The scenarios below integrate some of the basic building blocks needed as a starting position for the discussion of the architectural design (next step in the JRA5 roaming work item).

The scenarios provided in the AAI requirements document DJ5.2.1 were based on the following assumptions:

- Any user U is given an appropriate digital identity by his home institution HI.
- Digital identities issued by the HI are trusted and valid in a federation of participating institutions.
- In particular, if U wants to access or operate on resource R, his digital identity has to be trusted by the resource owner or service provider in the institution RI.
- The control of the authorisation to access or operate on a resource R is decided (or delegated) by an Authorisation Service of the resource owner or service provider at the institution RI.
- A mechanism exists that enables the exchange of authentication and authorisation information between the Authentication and Authorisation Services of HI and RI. This mechanism is part of a “Federation Service”.
- There is a federation-aware AAI component, called “Local Federation Connector”, which decides whether an authentication request can be handled locally or whether support from the Federation Service is needed.

In order to allow controlled inter-domain usage of resources, a harmonised digital identity concept is necessary between the AAIs of the federation partners. The RI AAI, for each potential guest, has to trust the identity management procedures and the Authentication Service in the corresponding HI AAI. Therefore, an identity federation has to exist with the RIs and the HIs as members. Furthermore, it is necessary that the Authorisation Service in the RI AAI is able to discover and communicate with the Authentication Service in the HI AAI. To

facilitate these two functions, the concept of the ‘Federation Service’ is introduced, and made available to the members of the federation. The federation service is a trust fabric that glues together the member AAls and provides the RI with a link to the users HI.

The resulting model can be easily applied to the roaming case seeing the network as resource R. All the assumptions made are still valid for network access.

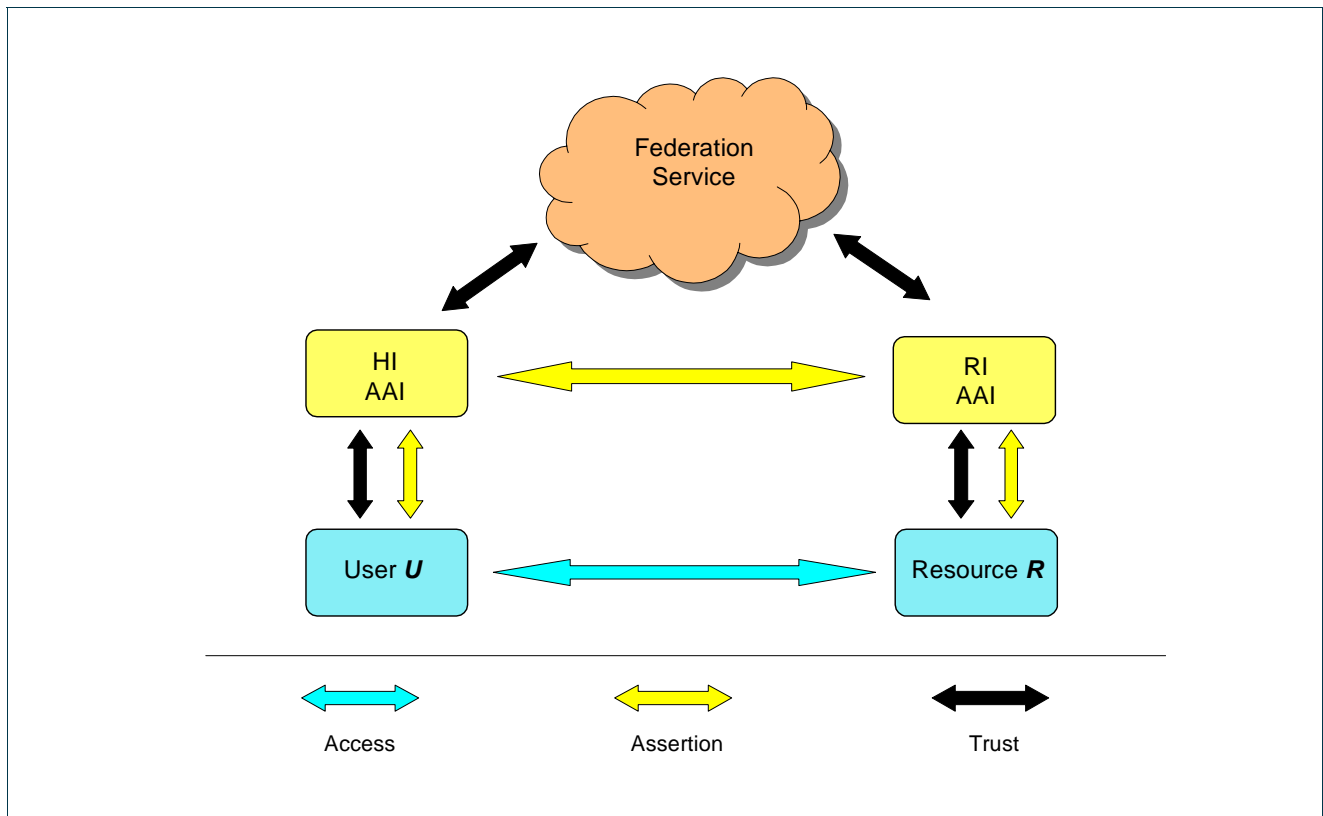


Figure 2-1: Federation Service as trust fabric between the home and remote AAI

## 2.2 The Network Access Scenario

The following scenario considers support for existing NREN-specific roaming solutions (as required), however these might not be federation-enabled. For that reason, a separate functional entity, called “Local Federation Connector” (LFC) is needed to connect to a federation to be established between non-federation-aware AA solutions. The LFC acts like a proxy-connector, performing all the required functions to enable inter-domain communication between existing AA systems. It is realized as a separate building block for conceptual reasons; in later implementations a combination of this functionality with closely related components, such as the Authentication Service, will probably be chosen if efficiency and performance advantages can be proven.

In this particular scenario user U, who has a valid digital identity at his home institution (HI), attempts to gain wireless network access as a guest at the visited institution VI. As the visited institution is the owner of the resource network it will be called Resource Institution (RI) from now on to preserve a common terminology with AAI. The HI and RI both are members of the network access federation provided. The following sequence of events is involved in the process of granting U access to the network (see also figure 2-2):

1. U associates with the wireless network access point at RI.
2. The access point considers this as a request for authorisation to use the network, and since U is not authenticated it asks U for his user identity, unique within the federation, and his encrypted identity credentials.
3. U sends his encrypted credentials, which can be decrypted by the Authentication Service at his HI only, and his digital identifier, "<U@HI>", to the access point.
4. The access point forwards the authentication request, the user identifier and the encrypted credentials to RI's Local Federation Connector (the federation service part at the visited institution).
5. The local authentication server, acknowledging the fact that it is not an authoritative authentication server for identities issued by the HI, forwards the request, the user identifier and the encrypted credentials to the Federation Service responsible for identifying and delivering the authentication request towards the HI.
6. The Federation Service forwards the request to the HI LFC.
7. The HI LFC forwards the request to the HI Authentication Service (HI AuthNS).
8. The HI AuthNS verifies the credentials and (after a positive result) sends back an authentication assertion.
9. The HI LFC forwards the assertion to the Federation Service.
10. The Federation Service sends the assertion to the RI LFC
11. The RI LFC forwards it to the access point.
12. The access point grants U access, and U has access to the wireless network from now on.

Note: Only steps 1 and 3 require an action (typing) from U, the other steps are processed automatically in the background.

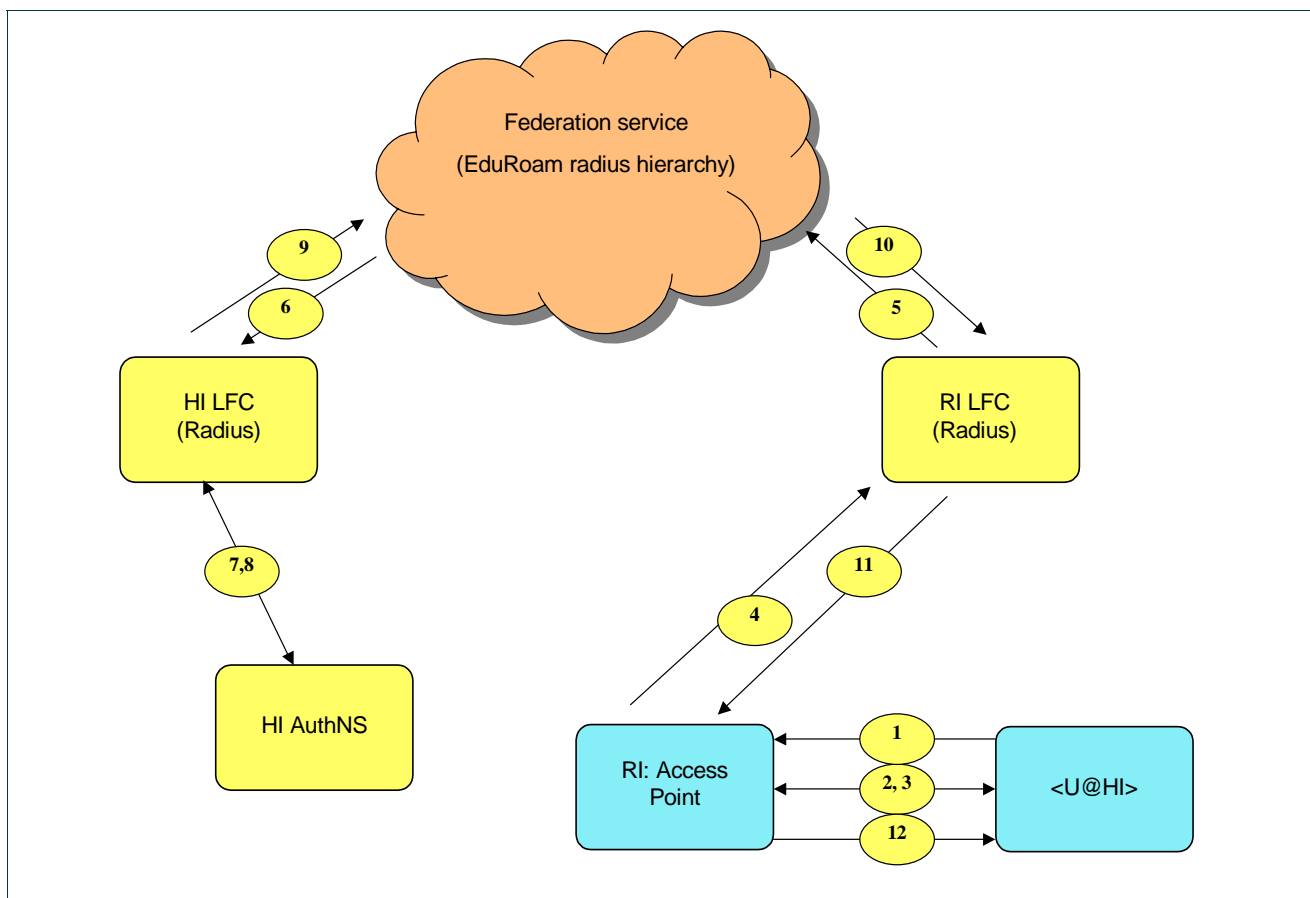


Figure 2-2: Communication pattern during network access control.

In the roaming infrastructure currently used (EduRoam) the authentication service is based on RADIUS servers. These are hierarchically interlinked and provide a simple form of a federation. Requests from users visiting RI can be forwarded via the top level RADIUS server to the HI authentication service. The assertion is sent the same way back.

## 3 General Requirements

This section presents general requirements for EduRoam-ng. The requirements discussed here are based on the requirements classes defined in DJ5.2.1 “Documentation on AAI Requirements”. They are influenced by the 2 years of practical experience with EduRoam.

The requirements are structured in several groups, starting with the general security requirements as the most important, followed by the standard compliance and finally by the operational requirements group.

The requirements are listed according to their relative importance within a group to accomplish the networking objectives in the current environment of academic networking. Indispensable requirements are indicated by “must”, nice-to-have requirements by “shall”.

### 3.1 Security Requirements

**Reasonable security:** The GÉANT2 roaming infrastructure EduRoam-ng must provide a sufficient level of trust to all participating partners (NRENs, institutions). The resources involved are the corresponding networks (backbones, campus networks, department networks) together with the docking network (based on wireless or wired technology) as part of the network infrastructure that shall be protected primarily. Granting network access must be available for authorised users only and shall not put unpredictable risks on the network provider.

**Data integrity:** EduRoam-ng must ensure the integrity of data transferred and processed in the entire infrastructure (user data, federated control information, payload). Providing confidence in the data integrity (users and administrators) is an essential element for establishing a fabric of trust in a distributed (and expandable) roaming infrastructure. To ensure the data integrity, a certain level of local maintenance is needed, in order to guarantee that only valid digital identities are used. A revocation procedure must be in place to handle cases of abuse by disabling rogue users. Some more (operational) aspects of data integrity will be covered in the operational requirements section.

**Compliance with privacy regulations:** When dealing with authentication and authorisation mechanisms, privacy becomes an extremely important area, both because of general public concern about this issue (specifically in the research and academic community), and because of the strict European and national regulations and general guidelines on privacy preservation (a dedicated documentation will be available later in the project). The infrastructure must avoid undesirable data leakage when performing AA interactions, and provide users with the ultimate control over what information about them is exchanged for what purposes. However, it may be helpful to point the roaming user to the local Acceptable Usage Policy (AUP) of the visited institution, if available.

**Verifiability:** The very nature of authentication and authorisation requires to keep a clear and end-to-end record of whom, when, what and why a given service was granted. The infrastructure shall be able to comply

with any legal requirements concerning AA-actions provided by the infrastructure. To which degree this might involve data protection issues will be discussed in the upcoming policy document (DJ5.1.3).

## 3.2 Standards Compliance and Integration

**Openness:** Building blocks and service elements of EduRoam-ng shall use open standard protocols and mechanisms to interconnect with other elements, either internal or external. This will allow for a simpler and faster integration of new components, and interoperability with existing or upcoming infrastructures, both in the academic, public and the commercial sector.

**Integration:** The pilot EduRoam infrastructure already in place provides a set of network access methods (IEEE 802.1X, web-redirect and VPN). The integrated approach will be based on these broadly distributed access technologies. EduRoam-ng shall be prepared to integrate new methods in a seamless way. The Local Federation Connectors (LFC) of EduRoam are currently based on a RADIUS technology. It should be possible to integrate other technologies, such as DIAMETER, Shibboleth or DNSSEC. EduRoam-ng should also be applicable to wired Ethernet "docking points" at visited institutions, that means 802.1X and the RADIUS infrastructure could be used for fixed network access as well.

Further more, integration with AAI is a very important requirement. An extension towards more qualified authentication and authorisation assertions is essential to pave the way for Single Sign-On (SSO). EduRoam-ng must be prepared to integrate existing AAI components or full infrastructures for example by offering gateway functionality.

## 3.3 Operational Requirements

**Scalability:** The infrastructure must be able to grow in several dimensions: geographically – spanning many countries/domains (nationally, internationally); functionally – integrating applications and services; structurally – reaching high integration with other regions/domains and reaching every end user/service. It must clearly scale to support a big number of sites and users at least on an European level (avoid problems of the  $n^2$  type), most likely world-wide.

**Ease of use:** It is a basic requirement for any middleware infrastructure to be as seamless as possible. This means that EduRoam-ng must impose minimum burden on both end users and administrators of services. No additional work shall be put on operators of authentication services or the staff defining and controlling the access policies to the network and to a certain set of resources. It must be easy to use for the roaming user, requiring at most a one-time set-up of client software (to be done at home), or even no special client set-up at all.

It is desirable to have a roaming solution available that could be used e.g. at events such as conferences that do not dispose a pre-installed roaming support. A quick and easy to install and to deploy software and a small number of devices (notebook, access points) should form a transportable roaming kit.

**Robustness:** An infrastructure like EduRoam-ng is a critical resource for any participating NREN. This implies that the infrastructure shall be able to sustain excessive strains on the system. This implies the existence of tools for infrastructure monitoring and test support.

## 4 Requirements on selected Building Blocks

In this section, specific requirements on building blocks for some entities of EduRoam-ng are defined. The architecture design is still under discussion, so this chapter is limited to functional buildings blocks that need to be provided independent from the final design.

The requirements are based on the following architectural assumptions:

- The EduRoam-ng will provide a superstructure, integrating existing and future NREN and/or campus roaming infrastructures;
- the superstructure will be based on a federation concept to facilitate interoperability between NREN roaming infrastructures and federated and autonomous national or regional roaming infrastructures;
- a federation agreement will specify the purpose and technical and business conditions of the federation;
- each federation member operates a Local Federation Connector (LFC) bridging the gap between the national (regional) roaming infrastructure component and the federation service.
- the EduRoam-ng will integrate seamlessly with the existing EduRoam pilot roaming service.

The requirements are also based on the assumption that a user shall only need to use one digital identity, provided and managed by the home institution, to access visited networks in Europe. It is however possible that a user possesses a number of digital identities associated with specific roles. Authentication and authorisation servers may use these role-based digital identities for finding decisions.

The chosen EduRoam-ng model is as follows: while authentication of the user is always done by the home institution HI, the authorisation to use the network resources are always controlled by the resource owner. The home institution of the user and the resource institution establish trust through the EduRoam-ng, and must

belong to at least one common federation. Federations are constructed for a special purpose. The parallel existence of more than one federation is not excluded.

## 4.1 Federation Service

EduRoam-ng shall contain a federation service for authentication and authorisation for network access. The purpose of this federation service is to act as a superstructure component that makes inter-organisational authentication and authorisation possible. For each single service (we assume to have more than one federation in parallel) there shall exist an agreement (federation document, see below) that gives (potential) members of the federation service and other relying parties sufficient information on which to base their level of trust in the service. The federation service shall preserve privacy during and after authentication, and it shall allow mutual authentication between the end-user U and the authentication server. Even though the particular service itself may be centralised, distributed or hierarchical, one institution shall be appointed to be the federation service provider for every single federation. The federation service provider acting on behalf of the education and research community is responsible for the operation and management of the service in accordance with the federation document.

The existence of a big number of federations with necessary co-ordination efforts between them can lead to scalability problems. The introduction of a hierarchy or of different trust levels might be useful and shall be considered at a later stage.

## 4.2 Local Federation Connector

For each member of a particular authentication or authorisation federation a Local Federation Connector (LFC) bridging the gap between the local EduRoam-ng component and the federation service shall exist. Within an authentication federation service the local EduRoam-ng component is the Local Authentication Service. The LFC is a component that discovers that the HI of the user to be authenticated is not the local one and takes care of redirect the authentication request to the appropriate authentication server at the HI. Within an authorisation federation service the LFC handles requests to locate the HI and get information about e.g. privileges and delegations that may have influence on the authorisation decision. The LFCs of different federation members need to communicate with each other and shall follow the specification of message formats and protocols given in the federation document.

## 4.3 Identity Management

The developed model for a federated authentication and authorisation service is based on the assumptions that the scope of a user identifier shall be the federation (i.e. the identifier is valid everywhere inside the federation), and that the concept and usage of a digital identity, as it is represented in the EduRoam-ng Identity Management concept, shall be harmonised within the federation. On the other hand, the choice of an appropriate authentication mechanism is in the responsibility of the HI, as long as the level of trust of that particular mechanism meets the conditions required to qualify as a member of the federation. The level of trust considered to be appropriate to be allocated to an asserted identity shall not only be based on the authentication mechanism used, but also on the routines for the Identity Management.

The precise meaning of "harmonised" identity and other information stored in user databases or directories is not defined here. One cannot assume that roles or authorisation attributes like student, member, faculty, working group etc have the same meaning in all partner institutions. An immediate requirement for all potential members in a JRA5 Identity Federation is that information about schemas, procedures for Identity Management, authentication mechanisms, and the format for assertions must be documented and made publicly available. A description of stored information about identities, such as categorisation of users, available for general authorisation, shall be specified and included as membership requirements in the federation documents.

## 4.4 Federation Documents

The evolution of trust between the members of a federation within EduRoam-ng shall be supported by the preparation of a "Federation Document". This document shall define a particular trust level by describing required routines and procedures around identity management and by defining required criteria for categorising users as e.g. member, staff etc. Membership in a federation shall be based on an authoritative declaration by each participating institution, committing to the required rules and procedures.

## 4.5 Authentication and Authorisation Mechanisms

There are a number of authentication mechanisms available and in use today; the decision which to choose and to provide to the user (dependent on the respective scenario) shall be made by the HI. Since the HI's decision on whether or not to permit network access has an impact on the RI (as the RI gives resources to the user), the RI may decide not to trust specific authentication methods even if the HI does, and consequently block all authentication attempts when a method that is considered unsafe is used.

Project:	GÉANT2
Deliverable Number:	DJ5.1.2
Date of Issue:	24/05/05
EC Contract No.:	511082
Document Code:	GN2-05-071v6

The U@HI presentation should be in the normal DNS format user@domain.tld. Internationalised Domain Names (UDN) can be used.

As a step towards implementing single sign-on, EduRoam-ng shall be designed to support both network-level and application-level authentication.

Credentials shall not be visible in a readable form by any component other than by the users own HI or by trusted software that is able to verify authenticity. The HI may however release other attributes of the user in accordance with the governing policies.

It is important for the user that the HI and the RI can agree on at least one method, which both of them trust, otherwise the user might not get access to the network even with valid credentials. Therefore it is important that one or more authentication methods can be used widely throughout the EduRoam-ng.

Out of the many authentication methods available today, those that transport credentials via an encrypted tunnel seem to provide a safe means of authenticating, as they authenticate both the user and the home institution, which makes identity-spoofing on both sides very hard.

While the assumption is that authentication of users is done by the authentication service in the HI, the authorisation of a particular operation on a resource is controlled by the institution of the resource owner (the RI). This control includes cases where the HI shall be asked whether it forbids or admits an authorisation request. An example for such a function is when the resource is expensive and the HI is requested to declare that it is willing to pay for the usage of the resource. In other cases, a user will directly be authorised by the resource owner.

EduRoam-ng shall be able to handle authorisation models supporting different levels/classes of access rights.

## 5 Conclusions

In the first 6 months of the project 3 deliverables have been produced: DJ5.1.1 Glossary of terms, DJ5.2.1 Documentation on AAI Requirements and DJ5.1.2 Documentation on Roaming Requirements. Hence, the general model is outlined and the terms to be used in this fast evolving research field have been defined. Some new terms have been added and a regular update of the glossary of terms is planned. Though the practical part of AAI and roaming is in a different stage of development, it was possible to imply the same general model and to keep the same requirements structure for both work items. This is a good starting point for SSO.

One important point to be added to the roaming requirements is the policy and legal framework. National and EU wide legal regulations have to be considered, and a recommendation for NRENs and for institutions participating in national roaming solutions shall be worked out. One part of this legal framework should be the provision of a federation document that covers the policy rules in EduRoam-ng.

The next steps to be taken in JRA5 will include the elaboration of the architectural design documents for both AAI and EduRoam-ng. The AAI architecture has to take into account the concepts of authentication and authorisation solutions already in place. Even though this will be a theoretical documentation it will be based on practical experiments in local testbeds of the partners. The roaming requirements defined in this document will be of influence on the design of the architecture; any AAI solution that does not obey these requirements shall clearly be avoided.