

01.02.05

Deliverable DJ5.2.1: Documentation on GÉANT2 AAI Requirements



Deliverable DJ5.2.1

Contractual Date: 31/12/04
Actual Date: 15/02/05
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: JRA5
Work Item: 2 (AAI)
Nature of Deliverable: R – Report
Dissemination Level: PU – Public
Lead Partner: RedIRIS
Document Code: GN2-05-026v6

Authors: T. Wiberg (NORDUnet, main editor), D. Lopez (RedIRIS), M. Milinovic (CARNet), J. Rauschenbach (DFN), K. Wierenga (SURFnet), with contributions from R. Castro (RedIRIS), T. Lenggenhager (SWITCH), M. Linden (NORDUnet), M. Molina (Dante), J. Sankar (Ukerna), D. Simonsen (NORDUnet), M. Sova (CESNET), S. Winter (RESTENA), H. Ziemek (DFN) and other GN2 groups

Abstract

The objective of this deliverable is to identify and to classify the requirements of the Authentication and Authorisation Infrastructure (AAI) that GN2 JRA5 is going to build to provide a federated solution for location-independent access to applications and services.

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

Table of Contents

0	Executive Summary	1
1	Introduction	2
2	AAI Scenarios	3
2.1	The generic scenario	5
2.2	Specific scenarios	5
2.2.1	Guest access to a network	6
2.2.2	Guest access to a web application	7
2.2.3	Use of shared computational resources	9
2.2.4	Guest access to electronic library	9
2.2.5	Project collaboration tools	10
3	General Requirements	11
3.1	Security requirements	11
3.2	Standard compliance and integration	12
3.3	Operational requirements	12
4	Requirements on selected building blocks	14
4.1	Federation Service	14
4.2	Local Federation Connector	15
4.3	Identity Management	15
4.4	Federation Documents	16
4.5	Authentication and Authorisation Mechanisms	16
5	Requirements of other GN2 Activities	17

Table of Figures

Figure 2-1: Federation Service as trust fabric between the home and remote AAI	4
Figure 2-2: Communication pattern during network access control.	7
Figure 2-3: Communication pattern during guest access to a web application	8
Figure 5-1: The AAI Service Model	18

0 Executive Summary

The objective of GN2 JRA5 is to develop a pilot service infrastructure for authentication and authorisation for the education and research community in Europe. This GÉANT2 Authentication and Authorisation Infrastructure (AAI) shall support seamless and location-independent network access to applications, services and other resources and provide authentication and authorisation services to other GN2 activities. As a first step, the requirements on the GÉANT2 AAI are outlined in this document.

It would be unrealistic to assume that our efforts could result in a homogenous infrastructure based on a particular method for authentication and authorisation. Our goal is rather a federation of autonomous AAIs, where the trust reasonable to have in a federation is indicated by the requirements on each member of the federation. The deliverable includes a generic scenario that illustrates the basic model of a federated AAI. The purpose of the federation service is to act as a superstructure component that makes inter-organisational Authentication and Authorisation possible. For two specific usage scenarios (network access, web access) the detailed sequence of steps in the authentication and authorisation process is presented. The pilot roaming authentication service "EduRoam" (www.eduroam.org) is included to demonstrate a real-life example of a federated AAI. It is useful for end users of academic networks, who can be granted guest access with minimum complexity for both users and administrators. Other scenarios are presented in short descriptions.

The general AAI requirements 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 categorised the general requirements into three major groups, listed in order of importance, as (1) Security, (2) Integration and standard compliance, and (3) Operation. Each group contains a set of requirements, also in order of importance. The more specific requirements in the document are related to known functional building blocks of an AAI. They will prove to be a useful reference to determine AAI characteristics and the architectural design.

Apart from defining the requirements related to the integrated GÉANT2 AAI, JRA5 will provide pilot installations of AA services for other GN2 activities. These are seen as specific cases, related to their requirements and needs. This deliverable will not only provide the basis for early AAI solutions, but will also serve as a mechanism for other JRAs and SAs to give feedback on JRA5 assumptions about their AAI requirements. This is to ensure that future AAI architectural design decisions can be based on a common infrastructure or at least that a feasible interoperable solution for GÉANT2 network access and service provision is created.

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

1 Introduction

The Authentication and Authorisation Infrastructure (AAI) that GN2 JRA5 is going to build is based on the vision that it will be used in academic institutions all over Europe, enabling seamless sharing of network and application resources. This GÉANT2 AAI shall provide authentication and authorisation services to other GN2 activities. The goal is to apply a set of harmonised AA practices within the GÉANT2 environment. The AAI shall be based on open standards and should be able to interoperate with similar infrastructures in the academic world. 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 authorisation.

JRA5 developments do not start from the ground up. They have to take into account location-independent network and service access and existing AA services, already established by NRENs and universities. 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 AAI solution, one must define interfaces for interoperability and create generic elements which can be further developed into services.

The first users of the infrastructure will be the members of JRA5. All necessary preparations will however be made to facilitate easy adoption by those NRENs, with their academic communities, that are not participating in JRA5 thus extend the user community further.

According to the JRA5 project plan, the GÉANT2 AAI shall initially be oriented towards application access (including the needs of other activities within the GN2 project) and will then be further extended to include location independent network access as the first step towards single sign-on (SSO) solutions. Web resource access and web services are application types of particular interest.

This document describes the requirements for the AA infrastructure to be built by JRA5. Chapter 2 contains a set of usage scenarios, showing the AA related interactions in typical application environments. Chapter 3 introduces the general requirements for the infrastructure, enumerating and analysing the criteria that the AAI shall meet in order to satisfy the needs for its intended use. Chapter 4 describes functional requirements, discussing first structural characteristics of the infrastructure. Finally, requirements from other GN2 activities are taken into account in chapter 5 and an initial service model is presented.

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

2 AAI Scenarios

The purpose of this chapter is to contribute to the requirements definition by illustrating the requirements on the integrated GÉANT2 AAI, thus providing both a generic usage scenario and a number of real-life usage scenarios from common everyday situations for researchers.

This project starts from a position where a number of AA solutions already exist, e.g. at institutional (campus) level, or at NREN level (spanning several institutions), all of which control users' access to resources based on authentication and authorisation information in their home institution HI. A typical scenario for currently used AA solutions could be described as follows: After the initial authentication by the Authentication Service, authorisation information about the user privileges are requested and provided to the resource-offering entity. This information is particularly necessary where different authorisation levels exist. In today's AA solutions, however, users and resources tend to belong to the same administrative domain which means that the user, the authentication and authorisation service and the resource provider locations are known and requests are passed to and from almost seamlessly.

Consequently, the problem that GN2 JRA5 has to solve, is the problem supporting multiple domains and variable authentication and authorisation systems and resource providers that may be in more than one domain. The requirement is to support a solution where a user U from a Home Institution HI wants to access or operate on a resource R in another domain RI, which owns the resource R (normally another NREN or institution belonging to the same federation). Therefore an AAI federation superstructure is needed, that knows where to send and receive requests across multiple federations and domains. The scenarios below show the basic building blocks needed as a starting position for the discussion of the architectural design (next step).

The scenarios provided in this document are 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.
- 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.
- 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.
- 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 local AAI. The RI AAI, for each potential guest, has to trust the identity management procedures and the Authentication Service in the corresponding HI AAI. Therefore, there needs to be an identity federation 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 AAI and provides the RI with a 'route' to the user's HI.

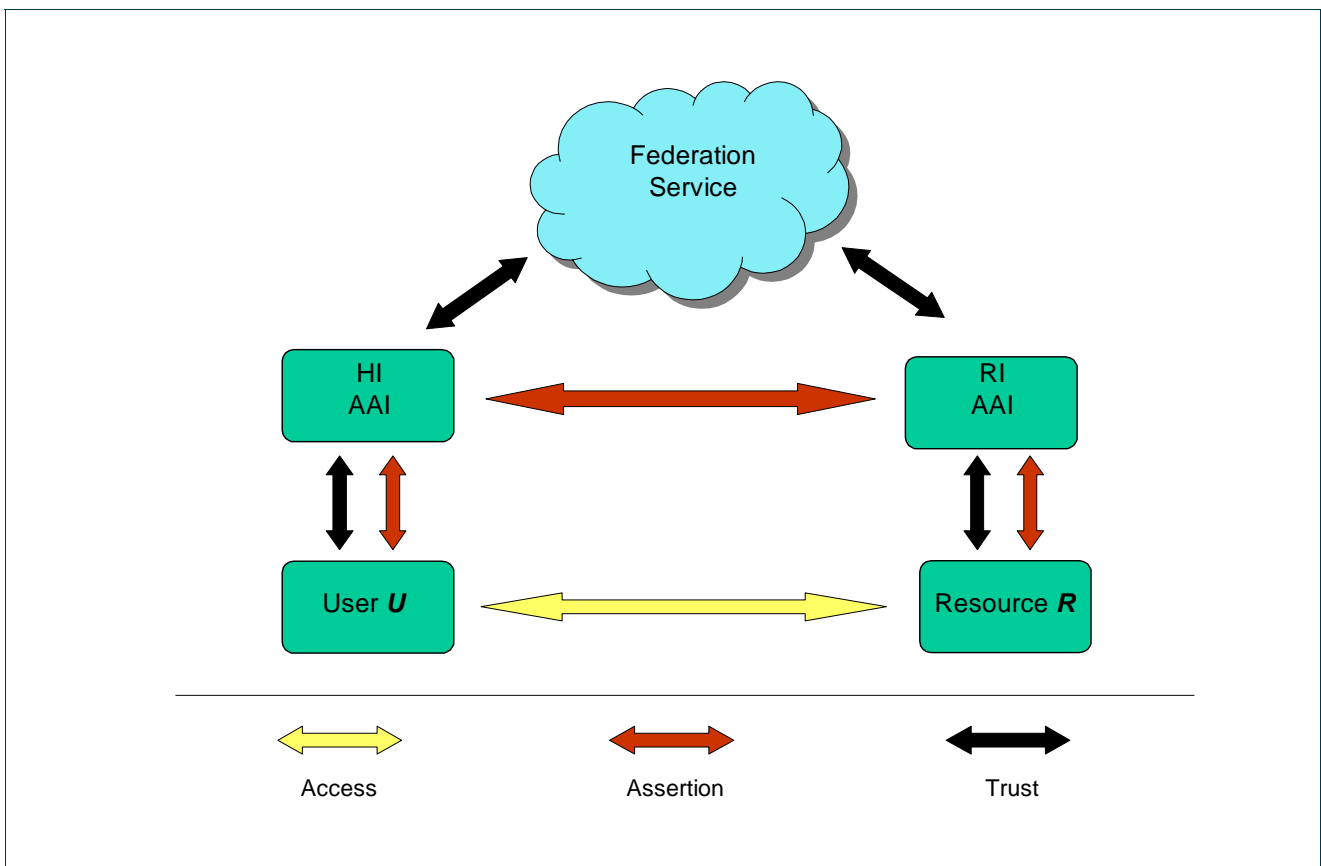


Figure 2-1: Federation Service as trust fabric between the home and remote AAI

2.1 The generic scenario

The generic scenario has evolved from the common situation where U, as a guest at a visited institution VI¹, wants to access or operate on a web accessible resource R. This scenario involves two authorisations: VI authorises U to use the network, and RI authorises U to access or operate on R.

Both of these authorisations can be mapped to the generic scenario:

The user U requests that RI authorises U to use the resource R. If U is not authenticated by HI yet, or a certain authentication level is needed, RI refers U to HI for authentication and possibly authorisation at the appropriate strength level. When RI can assert that U has been properly authenticated (and authorised), RI processes and responds to the authorisation request and provides the required access.

In the following sub-chapters this generic scenario is explained in more detail for two cases: network access to a roaming infrastructure and web access. Some more examples follow without detailed descriptions.

2.2 Specific scenarios

The example scenarios discussed in this chapter are related to a number of typical everyday situations, in which a future AAI could play a key role as enabler of inter-domain mobility from the viewpoint of authentication and authorisation. They are used to provide a broader scope of how the generic model described above could apply in specific situations.

All of the following scenarios in particular consider support for existing NREN-specific AA solutions (as required), however these usually do not possess the property of federation-awareness. For that reason, a separate functional entity, called “Local Federation Connector” (LFC) is introduced to enable 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.

¹ VI might be any institution in the federation, but to simplify, we will use VI = RI

2.2.1 Guest access to a network

In this scenario user U, who has a valid digital identity at his home institution (HI), as a guest at the visited institution VI attempts to gain wireless network access. The HI and VI both are members of the network access federation known as “EduRoam”. This means that in this scenario the network is the resource R and the VI thus is the resource institution RI, providing network access. 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 access point.
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 identity, “<U@HI>”, to the access point.
4. The access point forwards the authentication request, the user identity and the encrypted credentials to RI’s Local Federation Connector (the Federation Service part at the visited institution (which in the current version of EduRoam is a RADIUS server)).
5. This RADIUS server, acknowledging the fact that it is not an authoritative authentication server for identities issued by the HI, forwards the request, the user identity and the encrypted credentials to the Federation Service (EduRoam in this case) 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 he has access to the 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.

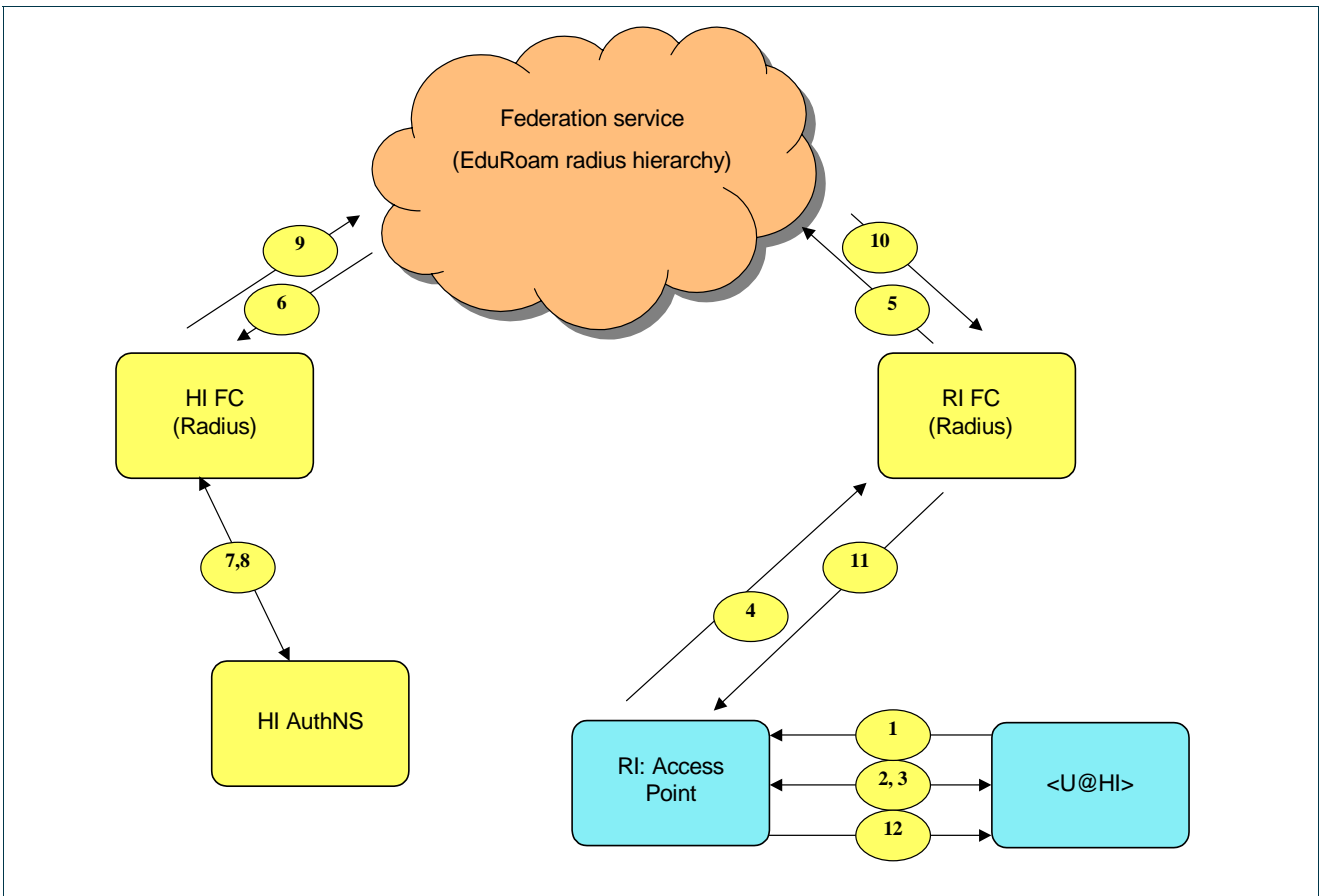


Figure 2-2: Communication pattern during network access control.

2.2.2 Guest access to a web application

In this scenario, user U, who has been authorised to use the network, tries to access a web page at a remote institution. In the general case he can do this being at RI or at another institution VI. The resource R in this scenario is the web page on a website at the remote Resource Institution (RI). The access to the website is controlled by an Authorisation Service at the RI (RI AuthZS).

U has a digital identity, issued by the HI. The RI AuthZS accepts a valid authentication assertion (e.g. an HTTP-token) from the HI to be one parameter to base its authorisation decision on. In typical current web-based access control systems, web redirects are used to control the access control flow.

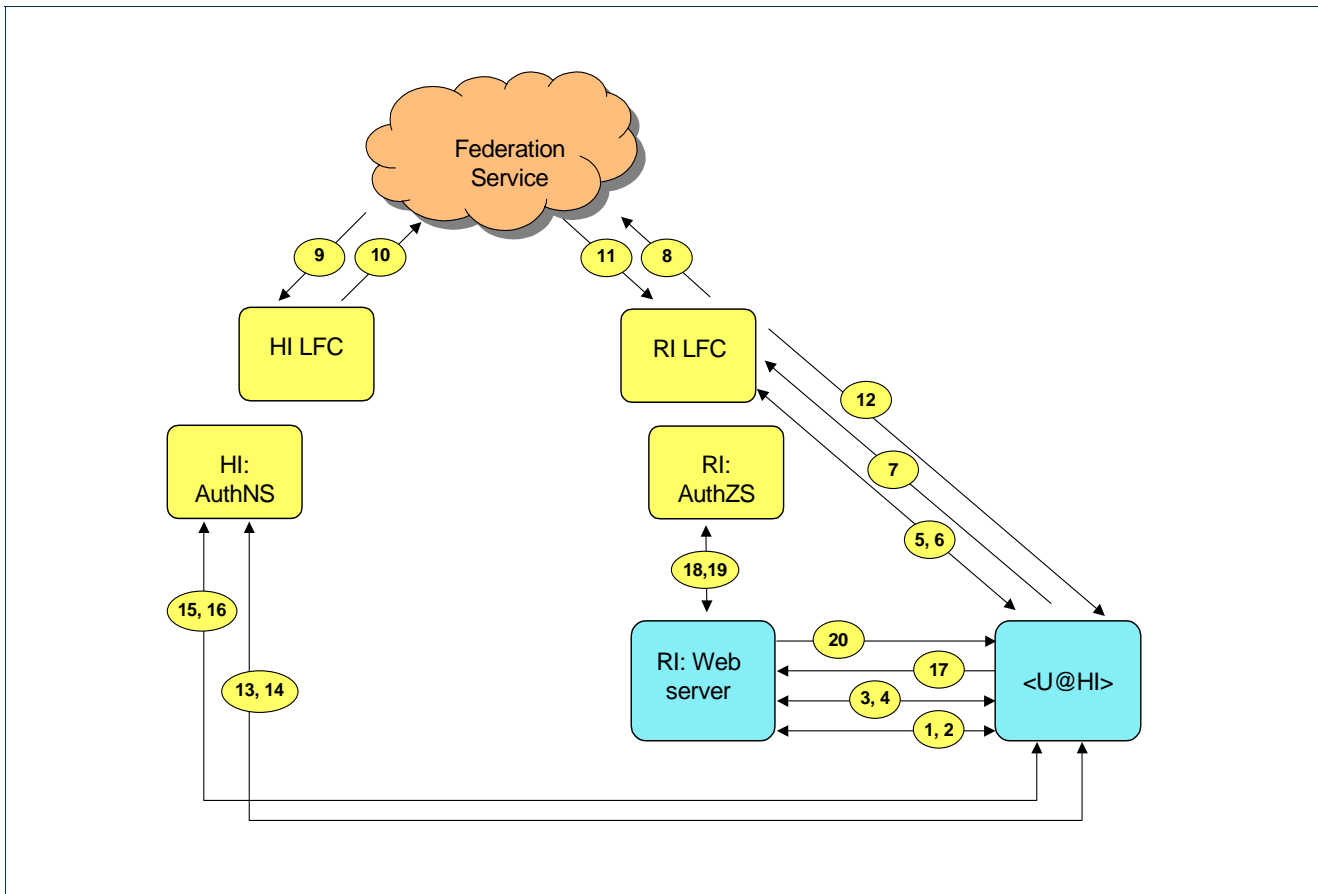


Figure 2-3: Communication pattern during guest access to a web application

1. U points his browser to a web page on a web server at the RI,
2. The web server, being the service access point of the resource, requests a valid authentication assertion, in this case an HTTP token such as a cookie, or a GET/PUT parameter.
3. U's web browser can not provide one.
4. The request is redirected to the RI Local Federation Connector, which is the federation-aware Authentication Service at the RI (RI LFC).
5. U's browser contacts the RI LFC.
6. The RI LFC asks U's browser for the HI.
7. The browser sends the @HI info.
8. The RI LFC, realising that RI does not have an authoritative AuthNS for a user from HI, asks the Federation Service to localise the HI LFC.
9. The Federation Service contacts the HI LFC.
10. The HI LFC replies with the location of HI AuthNS.
11. The Federation Service forwards this reply to the RI LFC.
12. The RI LFC redirects U's browser to the HI AuthNS.
13. U's browser contacts the HI AuthNS.

14. The HI AuthNS ask U for his digital identity credentials.
15. U presents the credentials.
16. The HI AuthNS authenticates U by issuing an authentication assertion (e.g. an http-token) and redirects U back to the RI web server.
17. U's browser hands over the authentication assertion to the RI web server.
18. The web server accepts the authentication and asks the RI Authorisation Service (RI AuthZS) if the user whose authentication assertion is stored in the http-token may access the requested web page.
19. The RI AuthZS returns an authorisation assertion to the web server.
20. U gets access to the requested web page.

In this example all logical steps are listed for a complete explanation. In a practical installation shortcuts might be possible to install.

2.2.3 Use of shared computational resources

User U wants to use the shared computational resources available through the grant from a national research council. The resources R are distributed over several institutions and provided by the members of a particular resource sharing federation. R is made available through a common Service Access Point (SAP) located at one of the institutions in the federation, RI. The allocation of fractions of R is controlled by a central policy, stating for example how the available resource shall be shared between users from the different research council communities. The central policy is enforced by the SAP through a Federated Authorisation Service.

After contacting the SAP and requesting access to R, U is authenticated by the HI using its normal identity credentials, as described in detail above. When the authentication is done and U has presented his authentication assertion to the SAP, U requests the allocation of the quantum of computational resources he wants. The SAP uses the local Authorisation Service to process the request. If the request satisfies the central policy, the request is forwarded to the relevant remote Authorisation Service through the LFC. If U's request satisfies the policy of the research council, the SAP is recommended to provide the requested resources.

2.2.4 Guest access to electronic library

U from the HI is visiting a university RI in another European country. He will attend a workshop where he and others shall give lectures, discuss scientific results and together go through quite a bit of new literature, helping each other to get a good overview of the latest news in their field of expertise.

At the meeting he acquires EduRoam-based network access by typing in his credentials as usual. Now he has access to the Internet like any other guest. On the basis of a stronger authorisation, based on a special contract, he might be able to upgrade to a higher service level. The first page he sees when he opens his browser after the upgrade is a local page from the RI telling him that as a visiting doctor from another EduRoam member, he has access to the web, the local printer as well as the sections, relevant to the workshop, in the electronic

library. He will now not only be able to search the local library but also to download the articles and print them out.

As a requirement the member universities of EduRoam would have to base the definition of their users on a common directory schema, e.g. euEduPerson (this is a hypothetical, currently non-existent directory service schema for employees in the GÉANT2 community). Then U, as a guest at RI, providing an attribute euEduPersonAffiliation, asserted by his HI and indicating “faculty from another member university”, will get access to the electronic library and to other resources.

2.2.5 Project collaboration tools

In a project such as GN2 JRA5, where the project members come from a large number of institutions and make smaller or larger contributions, project collaboration tools are the valuable means of making the tough job of synchronising the work of the members and securing adequate progress somewhat easier. To organise this, the GÉANT2 AAI can be used.

It is assumed that each member of the project team has a digital identity issued by an Identity Provider in their Home Institution. It is also assumed that the Identity Providers belong to the same Identity Federation. The resources in this scenario are the Virtual Office (in RI) with its collaboration tools: A document management system, a video conference system, a shared whiteboard, a shared application function, and a chat room function. User U requests access to the virtual office, by surfing to its Service Access Point (SAP). If U is unauthenticated he is redirected to the Local Federation Component and can eventually present the SAP with a valid identity assertion. The SAP admits U into the Virtual Office after verifying with the RI Authorisation Service that U is a member of the project team. Further authorities, once U has entered the Virtual Office, depends on his function in the project as it is described in the authorisation policy controlling what authorisation assertions the AuthZS might issue.

This chapter contains only a small set of possible scenarios from the research area. There exist a lot more, such as support for administration, eLearning etc. with varying requirements. The decision as to what specific scenarios will be taken into account initially in JRA5 will be made later in the project lifetime.

3 General Requirements

This section presents the general requirements for the GÉANT2 Authentication and Authorisation Infrastructure (AAI). The requirements discussed here can be considered a set of benchmarks for the achievements of GN2 JRA5, although the concepts around them are difficult to quantify accurately. It is also important to bear in mind that some of the requirements are inherently conflicting, making it necessary to build the final solution on a balanced compromise to achieve the overall best result. The requirements below are structured into several groups, starting with the general security requirements as the most important one, followed by the standard compliance and the operational requirements group. The requirements are listed according to their relative importance within a group and their relevance in the accomplishment of the infrastructure objectives in the current environment of academic networking. This classification is not an absolute, however, and may be subject to change in the future.

3.1 Security requirements

Reasonable security: The AAI shall offer carefully chosen trust and enforcement levels in accordance with different application or service needs. The motivation to consider deploying an infrastructure with a lower trust level (if at all) is the possibility of offering solutions with improved usability and performance, combined with a lower security. The GÉANT2 AAI shall provide a balance between carefully chosen security levels and usability and performance, always according to the nature of the protected resource in each case.

Data Integrity: The success of the federated AAI depends completely on data integrity of data securely transferred and processed within it. It must be ensured that the risk of data being tampered with during transmission or by unauthorised manipulation is in correspondence to the chosen trust and enforcement level. Trust in the data integrity is essential for establishing the federation as such, and is also crucial to attract new members to federations. To ensure data integrity, the data must be regularly maintained; revocations of credentials should be agreed at intervals that do not impair usability, and the security of the system, though aiming at a high performance, must be able to accommodate support for multiple authentication methods.

Compliance with privacy regulations: When dealing with authentication and authorisation mechanisms, privacy becomes an extremely important area, both because of general public and research and academic

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

community concerns about this issue, and because of strict European and national regulations on privacy preservation. The infrastructure must avoid unnecessary data leakage when performing AA interactions, and provide users with means to control over what information about them is exchanged and for what purpose.

Verifiability: The very nature of authentication and authorisation requires a strong capacity of keeping a clear and uniform end-to-end record of who, when, what and why a given service was granted. The infrastructure shall provide the necessary means to answer these questions when appropriate evidence about a certain interaction is requested.

3.2 Standard compliance and integration

Openness: Elements of the infrastructure shall use open standard mechanisms to interconnect with other elements, either internal or external, such as user applications, support mechanisms and other infrastructures. This will allow for a simpler and faster integration of new components, and interoperability with existing or future infrastructures in the academic, public and commercial sectors.

Integration: AA solutions are already, partially or fully, in place at a number of NRENs, universities and other higher education institutions with various applications using them for access control to resources or services. As a result, user communities and well-defined operating procedures exist. The GÉANT2 AAI must be able to offer integration of existing AA solutions or infrastructures at the appropriate trust level in the trust fabric. In order to do so JRA5 shall offer alternative migration or integration strategies, exploiting for example the possibilities of providing a *superstructure* with gateway functionality to extend their AA capabilities across federations and domains.

Neutrality: Since the infrastructure is aimed at incorporating different existing systems and will be used in a number of application domains, it is necessary not to mandate specific technologies at the edges of the infrastructure. This is because it could create problems in integrating local infrastructures and adapting applications willing to use it. Open and general interfaces shall be provided both internally (to connect local AA components) and externally (to connect applications).

3.3 Operational requirements

Scalability: The infrastructure shall be able to grow in several dimensions: regional – spanning many countries/domains; functionally – spanning many applications and services; structurally – reaching high integration with other regions/domains and reaching every end user/service.

Ease of use: It is a basic requirement for any middleware infrastructure to be as seamless as possible. This means that the AAI shall impose a minimum burden on end users and on administrators of services, like

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

operators of authentication services or the staff defining and controlling the access policies to a certain set of resources.

Robustness: An infrastructure like the discussed GÉANT2 AAI is a critical resource for any networked application. This implies that the infrastructure must be able to support excessive strains on the system in terms of high traffic load, relatively uncritical network disruptions and even deliberate attacks without catastrophic results.

Flexibility: The infrastructure shall allow each of the actors interacting and/or using it to manage and enforce their own policies. This includes authenticators and identity providers, service providers, user communities, etc. The basic principles of federated administration, allowing for the de-coupling of procedures by means of the establishment of a web of trust among the actors are to be applied here.

4 Requirements on selected building blocks

In this section, specific requirements on building blocks for some entities of the resulting integrated GÉANT2 AAI for e-science activities in Europe are defined.

These requirements are based on the following architectural assumptions:

- The GÉANT2 AAI will provide a superstructure, integrating existing and future NREN and/or campus AAI (here denoted local AAI);
- the superstructure will be based on a Federation concept to regulate and technically specify the means of harmonising the autonomous local AAI;
- a Federation Agreement will specify the purpose, technical and business terms of the Federation;
- each Federation and Federation member owns a Local Federation Connector (LFC) bridging the gap between the Local AAI component and the Federation Service constituting the corresponding superstructure component.

The requirements are also based on the assumption that a user shall only need one digital identity², provided and managed by the Home Institution, to conduct the different e-science activities in Europe. The chosen AAI model is as follows: while Authentication of the user is always done by the Home Institution, the Authorisation to use or operate on the resources involved in the users activities are always controlled by the resource owner.

4.1 Federation Service

The GÉANT2 AAI shall contain a Federation Service for Authentication and Authorisation. 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

² In case a user has different roles different digital identities might be needed

shall exist an agreement (Federation Document) 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 support web-based authentication and authorisation, and at least provide one model implementation of non-web-based (e.g. application or network) authentication. Even though the particular service itself may be centralised, distributed or hierarchical, one institution shall be appointed to be the Federation Service Provider. The Federation Service Provider 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 Federation for Authentication or Authorisation that is contributing to the Service, there shall be a Local Federation Connector (LFC) bridging the gap between the contributing Local AAI component and the Federation Service. For a Federation Service for Authentication, the Local AAI component is the Local Authentication Service and the LFC is a component that discovers that the HI of the user to be authenticated is another and takes care of that. For a Federation Service for Authorisation the LFC shall take care of requests to locate and get information about, for example, privileges and delegations that may have influence on the authorisation decision. The LFCs 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 globally valid inside the Federation), and that the concept and usage of an identity, as it is represented in the AAI's Identity Management concept, shall be harmonised over the federation. On the other hand, the choice of authentication mechanism shall be a matter only for the Home Institution, as long as the level of trust for 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.

Thus, the precise meaning of "harmonised" identity and other information stored in user databases or directories is not defined here, but a first requirement on all potential members in a JRA5 Identity Federation is that information about schemas, procedures for Identity Management, authentication mechanisms, and the format for assertions are 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 the AAI shall be made easier by the development of a 'Federation Document'. The document shall define a particular trust level by describing the required routines and procedures around identity management and by defining the required criteria for categorising users in for example faculty, staff etc. Membership in a federation shall be based on an authoritative declaration by the institution that it commits to the requirements in the document.

4.5 Authentication and Authorisation Mechanisms

There are a number of authentication mechanisms available and in use today; the decision about which to choose and to provide to the user (dependent on the respective scenario) shall belong to the HI.

As a step towards implementing Single Sign-on, the AAI shall be designed to support both network-level and application-level authentication. Amongst the supported application authentication mechanisms, secured web-based authentication and a non-web-based authentication mechanism shall be implemented.

Credentials shall not be visible in a readable form by any other component other than by the user's own HI or by trusted software that is able to verify authenticity. That could also be a Java Applet, some local client or plug-in of some form which takes the credentials and encrypts them.

A set of common schemes for authority and identification information shall be defined as a basis for the AAI; a first step could be to agree on and use a European extension of the eduPerson and eduOrg directory objectclasses. A common, well-defined syntax and semantics shall be chosen or developed for communicating explicit entitlements and for attribute values available for authorisation. An effort shall be made to characterise authority concepts for classes of applications in order to simplify the development of authorisation policies.

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.

The AAI shall be able to handle authorisation models supporting different levels/classes of access rights.

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6

5 Requirements of other GN2 Activities

The JRA5 group has recognized the need for a prompt coordination with other activities within GN2 that will require the support of authentication and authorisation services. Early contacts have been made with SA3: End to End Quality of Service, JRA1: Performance Monitoring and Management and JRA3: Bandwidth on Demand. Although it is a little bit premature to consider the results of these contacts as formal requirements, the initial answers from these other activities include:

- The need to consider not only humans but also machine-based agents or elements as the users of the AAI.
- The possibility of (hierarchically) grouping individual users into one or more groups with associated policies.
- Support for multi-domain operation.
- User applications envisage to employ both authentication and authorisation services.
- The AAI will allow the use of external checks: Once a user has demonstrated to belong to an appropriately authorised group, additional checks may be necessary to evaluate whether it is possible to execute the requested action in the exact moment when it has been requested.
- Federation services should be easily extended to new members. Although details are not agreed yet, the usage of PKI is the most feasible option.

JRA5 has elaborated an initial service model by proposing the concept of a Service Access Point (SAP) as the inter-domain service abstraction. An SAP will exist at least per domain and service, and will be used by the requesting user/domain and the providing domain(s) to negotiate service provision. The SAP at each domain will use its local AAI instance to evaluate user identity, attributes and rights, according to the agreed service policies.

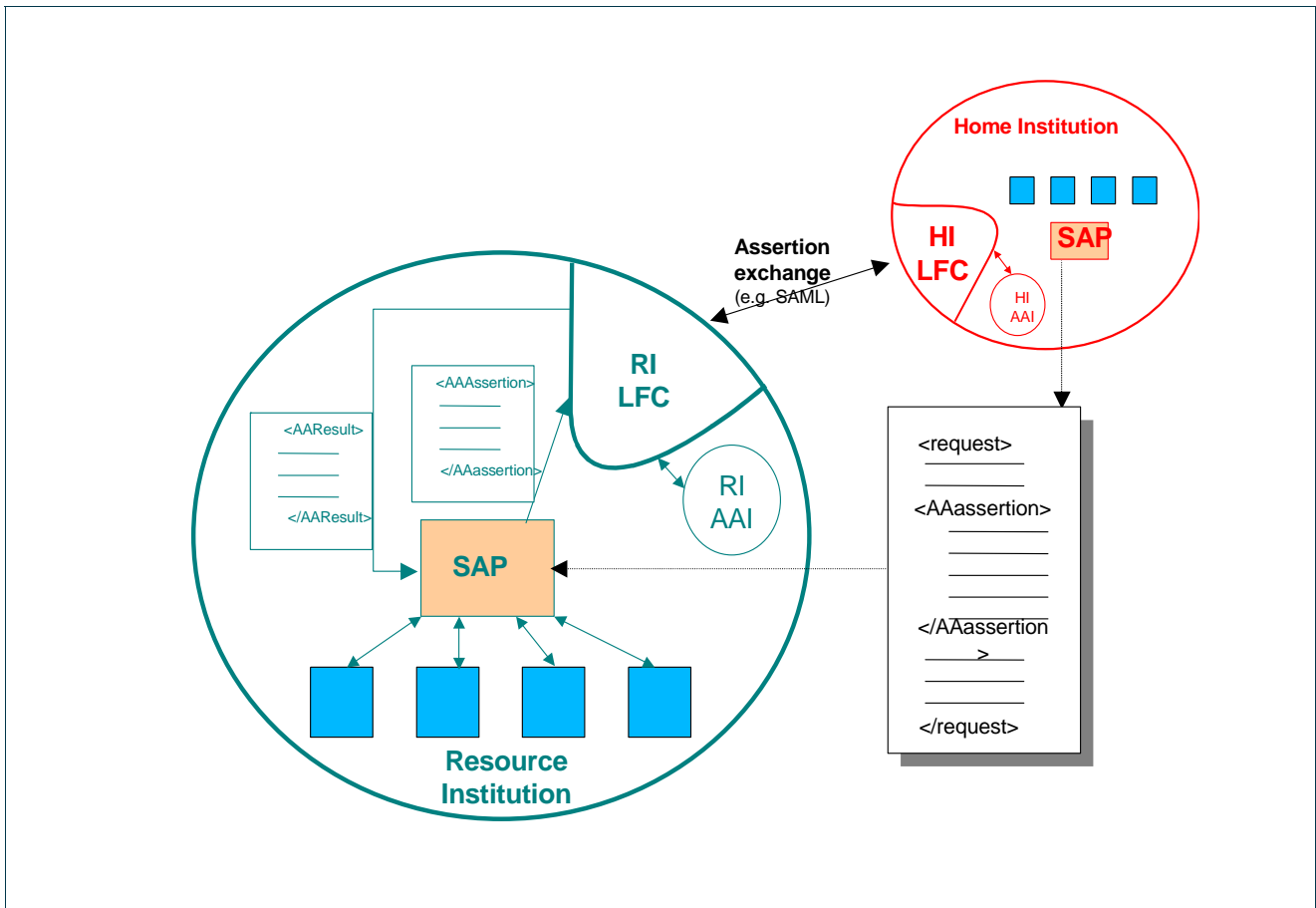


Figure 5-1: The AAI Service Model

This service model (depicted in the picture above) has been initially forwarded to the above-mentioned GN2 areas, leading to promising results pointing to a common understanding of the trust fabric for the provision of network services within GÉANT2.

Project:	GÉANT2
Deliverable Number:	DJ5.2.1
Date of Issue:	15/02/05
EC Contract No.:	511082
Document Code:	GN2-05-026v6