

13.03.07

## Deliverable DS3.14.1: GÉANT2 Identity Provider (GIdP) Design



### Deliverable DS3.14.1

Contractual Date: 28/02/07  
Actual Date: 09/03/07  
Contract Number: 511082  
Instrument type: Integrated Infrastructure Initiative (I3)  
Activity: SA3  
Work Item: 14.1  
Nature of Deliverable: R  
Dissemination Level: PU (Public)  
Lead Partner: SWITCH  
Document Code: GN2-06-326v7

**Authors:** Thomas Lenggenhager (SWITCH), Diego Lopez (RedIRIS), Javi Masa (RedIRIS), Maurizio Molina (DANTE), Christoph Witzig (SWITCH)

### Abstract

This deliverable specifies the architecture and design for the GÉANT2 Identity Provider, an eduGAIN compatible Identity provider for early users of GN2 services.

# Table of Contents

0	Executive Summary	iv
1	Service Description	1
1.1	Motivation	1
1.2	Implementation Overview	1
1.3	Roadmap and Duration	2
1.4	GIdP Activity Container	2
2	Requirements and General Design	3
2.1	GIdP Administration	3
2.2	Support for User Differentiation	4
2.2.1	Role of the User	5
2.2.2	Project or Scope the User belongs to	5
2.2.3	Home Network Domain of the User	7
2.2.4	Identity and Contact Information	7
2.2.5	Mnemonic (or opaque) Login Name	8
2.2.6	Other Attributes	8
2.3	Robustness and Availability of GIdP Service	8
3	Architecture	9
3.1	The eduGAIN Architecture	9
3.2	The GIdP Architecture	10
3.2.1	The Delegation Model for the GIdP Administrators	12
3.3	The Role of the GIdP User Administrator Managing GIdP User Entries	13
3.4	GIdP Administrator Web Application	13
3.4.1	Basic Features	14
3.4.2	Extended Features	14
3.5	Migrating Users from the GIdP to their Institutional IdP	15
4	GIdP Rules	16
4.1	GIdP Usage	16
4.2	Obligations	17

4.2.1	GIdP Service Provider (DANTE)	17
4.2.2	GIdP Service Administrators	17
4.2.3	GIdP User Administrators	17
5	Software to Use	19
5.1	IdP Component	19
5.2	GIdP Administrator Web Application	19
6	Hardware Needs	20
6.1	Basic Hardware to Start with	20
6.2	Extended Hardware for full Service	20
7	Dependencies & Next Steps	21
8	Conclusions	22
9	References	23
10	Acronyms	24

## Table of Figures

Figure 3.1: The eduGAIN architecture	9
Figure 3.2: An example of eduGAIN usage to provide AA to perfSONAR resources	10
Figure 3.3: The GIdP architecture	11

## 0 Executive Summary

The GÉANT Identity Provider (GIdP) will be a central common Identity Provider for early adopters of GN2 services whose home institution and NREN level Authentication and Authorisation Infrastructure (AAI), if available at all, is not yet connected to eduGAIN.

The GIdP helps to solve the 'chicken and egg' problem when using the eduGAIN AAI to protect access to GÉANT2 services and resources. The GIdP should become obsolete once eduGAIN spans all NRENs, i.e. when all users of services offered via eduGAIN have a home institution which is eduGAIN enabled.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

# 1 Service Description

## 1.1 Motivation

Several Joint Research Activities and Service Activities within GÉANT2 require Authentication and Authorization (AA) for controlled access to resources like

- measurement data for perfSONAR
- a Premium IP Service for AMPS, or
- a Domain or Inter-Domain Manager for setting up L1, L2 or MPLS circuit, for JRA3.

JRA5 is developing a federated AA Infrastructure (AAI) called “eduGAIN”, and SAs and JRAs will exploit it. There is already ongoing coordination between some of these activities and JRA5 to ensure that eduGAIN can fulfil the activities’ requirements.

EduGAIN was conceived to leverage existing AAI already in place in NRENs. But not all of the users of GÉANT2 activities may belong to institutions that have an AAI service, and even if they do, it may take considerable time before their AAI is extended to be eduGAIN compatible. This will prevent users (in particular early adopters) from accessing systems developed by GÉANT2 activities. Temporarily disabling AA functionality in such systems is not an option, since even in the pilot phase they are providing access to sensitive data and resources, like performance measurement results or Premium IP bandwidth.

The GÉANT2 Identity Provider (GIdP) should become a GN2 centralised common Identity Repository for:

- early adopters of services developed within the GÉANT2 activities (e.g. perfSONAR, AMPS), without waiting that their (existing) institution and NREN level AAI is connected to eduGAIN;
- adopters of services developed within these activities, whose institution has not deployed an AAI, or whose servicing NREN has not deployed an NREN level AAI;

## 1.2 Implementation Overview

The GIdP will be a special instance of an Identity Provider operated by DANTE on behalf of the users who do not have the possibility to get access to GÉANT services relying on the digital identity provided by their home institution. Users who get a digital identity from the GIdP are called 'GIdP users'.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

To be eligible to become a GIdP user, the person has to be affiliated to a home institution which itself belongs to the constituency of an NREN or a similar institution (like DANTE or TERENA)<sup>1</sup>.

GIdP user administrators from NRENs will be responsible for registering the GIdP users belonging to their constituency (NRENs). DANTE will request from the NRENs to nominate GIdP user administrators.

The idea for establishment of a GIdP is based on the SWITCHaai Virtual Home Organisation [VHO], which proved very useful for solving the 'chicken and egg' problem for bootstrapping services while not all Identity Providers are established.

### 1.3 Roadmap and Duration

The GIdP is expected to be an interim service for a duration of several years, until all NRENs have deployed eduGAIN compatible AAls with full coverage of their constituencies.

The earliest activity milestones and deliverables, in chronological order, are the following:

- Jan 07: *GIdP Policy Definition*  
Includes the definition of the attribute model and the support for the eduGAIN trust model.
- Feb 07: *GIdP design*, this document  
Includes the architectural design, the definition of the policies for user registration and user attribute assignments, and the definition of the trust model between the system administrator, the user administrators and the resource owners.
- Jun 07: *GIdP installation*  
Deployment of HW and SW infrastructure.
- Jul 07: *GIdP Pilot*  
Registration of a first user group and connection tests with service.

### 1.4 GIdP Activity Container

GIdP is a Work Item in SA3 ("Introduction of Multi-Domain Services"). Participating organisations are DANTE, SWITCH and RedIRIS. The wiki page of the activity, containing all working material, is [SA3-Wiki].

---

<sup>1</sup> 'NREN or similar institution' is elsewhere in this document just called NREN.

## 2 Requirements and General Design

Requirements and general design must consider the following aspects:

- administration of the GIdP;
- support for user differentiation (including the attributes as requested by the projects that want to use GIdP);
- robustness and availability of the service.

### 2.1 GIdP Administration

The GIdP is a repository of identity and attributes of users of GÉANT services, whose purpose is to be useful (and therefore “trustworthy”) for the largest possible base of providers of such services<sup>2</sup>. Therefore, a balance must be found between a very “centralised” and a very “distributed” identity verification and registration process. A centralised approach has the advantage of increasing trust in the repository (all the service providers just have to trust one authority and the way it operates) but creates a central bottleneck, and the registration and identity verification process may become lengthy and cumbersome. A very distributed approach has the advantage of making the registration process quicker and more feasible, but has the drawback of reducing the overall trust in the repository, because the service providers have to trust a large number of registration authorities.

The requirement, for GIdP, is to set this balance at the NREN level, i.e. to have one authority per NREN responsible for user registration. These authorities can further delegate the registration, but remain responsible for the correct behaviour of whom they delegate. Therefore, each GIdP user **MUST** be related to one of the NRENS and his corresponding digital identity is managed by the GIdP user administrators of that NREN.

The registration authorities **MUST** implement some form of verification of the user identity they register, therefore a simple self-registration based on web forms filling is not acceptable. The level of assurance for the identity vetting **MUST** follow the current practice of the NREN.

---

<sup>2</sup> Elsewhere in this document called “Resource Owners”

There **MUST** be some guarantee that the access credentials are communicated to the actual registered person, e.g. by calling an office phone number or by sending an e-mail to an address with a known and trusted “domain” part, belonging to the organisation of the registered user. When the credentials are communicated by e-mail, they **SHOULD** be sent encrypted with a public key advertised on a public or company key server. When the above is not possible, the method used to communicate the access credentials can follow the current practice of the NREN, although communications of credentials via non-encrypted e-mail is discouraged.

An NREN must be able to investigate cases of misuse/abuse of resources originating from user accounts registered by its registration authority, when such circumstances are self-discovered or signalled to the NREN by external authorities. The action may involve the removal of some user accounts. There **MUST** be a way to temporarily block the suspected user accounts even before the investigation is terminated. There **MUST** be a GIdP service administrator<sup>3</sup> capable of promptly enforcing this blocking if urgency is needed or the NREN level registration authority does not react promptly.

The registration authorities **SHOULD** be able to extend the attribute set of users after their creation. In particular, they should be able to add specific attribute values that some service providers may require to authorize users' resource access. Some service providers may in fact not judge the repository trustworthy enough, and may want to give access only to users they directly trust. Letting service providers directly add users (or modify their attributes) to the repository would however cause too much problems and move the model too much towards “distributed” registration. Therefore, the requirement is that the registration authority (at the NREN level) is capable of promptly reacting to service provider requests about the addition of resource specific attribute values to specific users. When doing so, the registration authorities **MUST** ensure that

- The requesting service provider has the right to place such a request;
- That the modification does not conflict with the capability of the user to access services other than the one the modification is made for.

## 2.2 Support for User Differentiation

These requirements are relevant for the whole eduGAIN, not limited to GIdP. However, the GIdP service in particular has to fulfil the resource owners' needs.

Role-based authorization means authorizing users on the basis of commonly agreed characteristics that can be recognised and understood by the resources for which authorization is sought. These characteristics are mapped into user attributes schemas.

---

<sup>3</sup> The exact role of the GIdP service administrator is described in 3.2

The user's attributes must be sufficient to perform role-based authorization for the supported GÉANT services. Since some of those services will be offered to a wide range of user profiles (e.g. both NREN NOC engineers and end users, like academic staff) this will possibly require extending existing schemas (e.g. eduPerson [eduPerson], SCHAC [SCHAC]) to incorporate differentiation among roles not yet covered by the current schemas' definitions.

The syntax and semantics of attribute values MUST be clearly described. GIdP MUST use only attributes that are acceptable within eduGAIN.

Furthermore, specific attribute values MAY be added upon service providers request, for specific users (see 2.1 above).

The attributes considered here are designed to contain information specifically about people. It is helpful to categorize this information. The categories used in this document have been collected from attribute requirements for GIdP's registered users received from SA3 (AMPS), JRA1 (perfSONAR), JRA3, SA3 (cNIS) and JRA4.

The six categories are:

- Role of the user
- Project the user belongs to, together with their project specific role in it
- Home network domain of the user
- Identity and contact information
- Mnemonic (or opaque) login name
- Other attributes

## 2.2.1 Role of the User

### 2.2.1.1 *schacPersonalPosition*

This attribute is used to store what the user does (a real personal position) within an organization.

References: SCHAC-IAD v: 1.3.0, section 4.4.1  
<http://www.terena.org/activities/tf-emc2/docs/schac/schac-schema-IAD-1.3.0.pdf>

Example: urn:mace:terena.org:schac:personalPosition:gr:ntua:noc:head

## 2.2.2 Project or Scope the User belongs to

In order to store information related to the user roles inside specific projects and names of these projects, two attributes in the SCHAC schema will be used.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

At the moment of writing this document these attributes are still experimental. They have been defined below an experimental branch and they will be proposed to be included in the next SCHAC release.

The attribute meta-information and notation used for these attributes are:

### 2.2.2.1 *schacProjectMembership*

Name: schacProjectMembership  
Description: The name of the project  
Format: urn:mace:terena.org:schac:projectMembership:<project-name>  
The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at <http://www.terena.org/registry/terena.org/schac/projectMembership/>  
# of values: Multi  
RFC 2252 definition: ( schacExpAttr:1  
NAME 'schacProjectMembership'  
DESC 'Name of the project'  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )  
Example: urn:mace:terena.org:schac:projectMembership:perfsonar

### 2.2.2.2 *schacProjectSpecificRole*

Name: schacProjectSpecificRole  
Description: Used to store a set of roles inside specific projects  
Format: urn:mace:terena.org:schac:projectSpecificRole:<project-name>:<iNSS>  
The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at <http://www.terena.org/registry/terena.org/schac/projectSpecificRole/>  
<iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive  
<project-name>  
# of values: Multi  
References: RFC 2141 - URN Syntax  
RFC 2252 definition: ( schacExpAttr:2  
NAME 'schacProjectSpecificRole'  
DESC 'Name of the project'  
EQUALITY caseIgnoreMatch  
SUBSTR caseIgnoreSubstringsMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )  
Example: urn:mace:terena.org:schac:projectSpecificRole:perfsonar:developer

## 2.2.3 Home Network Domain of the User

### 2.2.3.1 *schacHomeOrganization*

User's home domain (domain name according to RFC 1035, only one value for each user)

References: SCHAC-IAD v: 1.3.0, section 4.2.1  
<http://www.terena.org/activities/tf-emc2/docs/schac/schac-schema-IAD-1.3.0.pdf>

Example: tut.fi

### 2.2.3.2 *schacHomeOrganizationType*

Type of a Home Organization

References: SCHAC-IAD v: 1.3.0, section 4.2.2  
<http://www.terena.org/activities/tf-emc2/docs/schac/schac-schema-IAD-1.3.0.pdf>

Examples: *Common values:*  
urn:mace:terena.org:schac:homeOrganizationType:int:university  
urn:mace:terena.org:schac:homeOrganizationType:int:uas  
urn:mace:terena.org:schac:homeOrganizationType:int:research-institution  
urn:mace:terena.org:schac:homeOrganizationType:int:university-hospital  
urn:mace:terena.org:schac:homeOrganizationType:int:nren  
urn:mace:terena.org:schac:homeOrganizationType:int:other

*National extensions:*  
urn:mace:terena.org:schac:homeOrganizationType:ch:vho  
urn:mace:terena.org:schac:homeOrganizationType:es:opi

## 2.2.4 Identity and Contact Information

GÉANT activities need to know the identity of a user only in case of abuse or misbehaviour. That is, identity and contact information is not meant to be useful for authorization purposes, and must not be transferred from the GIdP to the service provider unlike the other attributes. But this information **MUST** be stored in the GIdP and it **MUST** be possible to relate it with the mnemonic (or opaque) login name described below in 2.2.5. The format in which identity and contact information is stored is not specified, and it will be up to the single GIdP user administrator to provide enough detail to identify (and contact) the user.

## 2.2.5 Mnemonic (or opaque) Login Name

Attributes relative to the login of the user.

### 2.2.5.1 *eduPersonPrincipalName*

The "NetID" of the person for the purposes of inter-institutional authentication. Should be stored in the form of `user@univ.edu`, where `univ.edu` is the name of the local security domain.

Note that the "user" part may or may not be something related to the user's real name.

In the realm of GIdP, the local security domain is the GIdP itself. Therefore, all GIdP users will have values in the GIdP domain.

References: [internet2-mace-dir-eduPerson-200604](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html), section 2.2.8  
<http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html>

Examples: `hputter@gidp.geant2.net`  
`a129b232@gidp.geant2.net`

## 2.2.6 Other Attributes

The use of `eduPersonEntitlement` is recommended to store specific access or use rights that are not covered by the previously defined attributes.

### 2.2.6.1 *eduPersonEntitlement*

URI (either URN or URL) that indicates a set of access or use rights to specific resources.

References: [internet2-mace-dir-eduPerson-200604](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html), section 2.2.2  
<http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html>

Examples: `http://xstor.com/contracts/HEd123`  
`urn:mace:washington.edu:confocalMicroscope`

## 2.3 Robustness and Availability of GIdP Service

GIdP MUST support at least 1.000 users, with a single database backend. The user database backend SHOULD be replicated. The support of the server(s) hosting the GIdP will be similar to the one of other DANTE's servers delivering production services.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

## 3 Architecture

### 3.1 The eduGAIN Architecture

The eduGAIN architecture is fully described in DJ5.2.2 [AAIarch], and in the (not yet published) DJ5.2.2 bis [AAIarchbis]. Hereafter is just a quick summary.

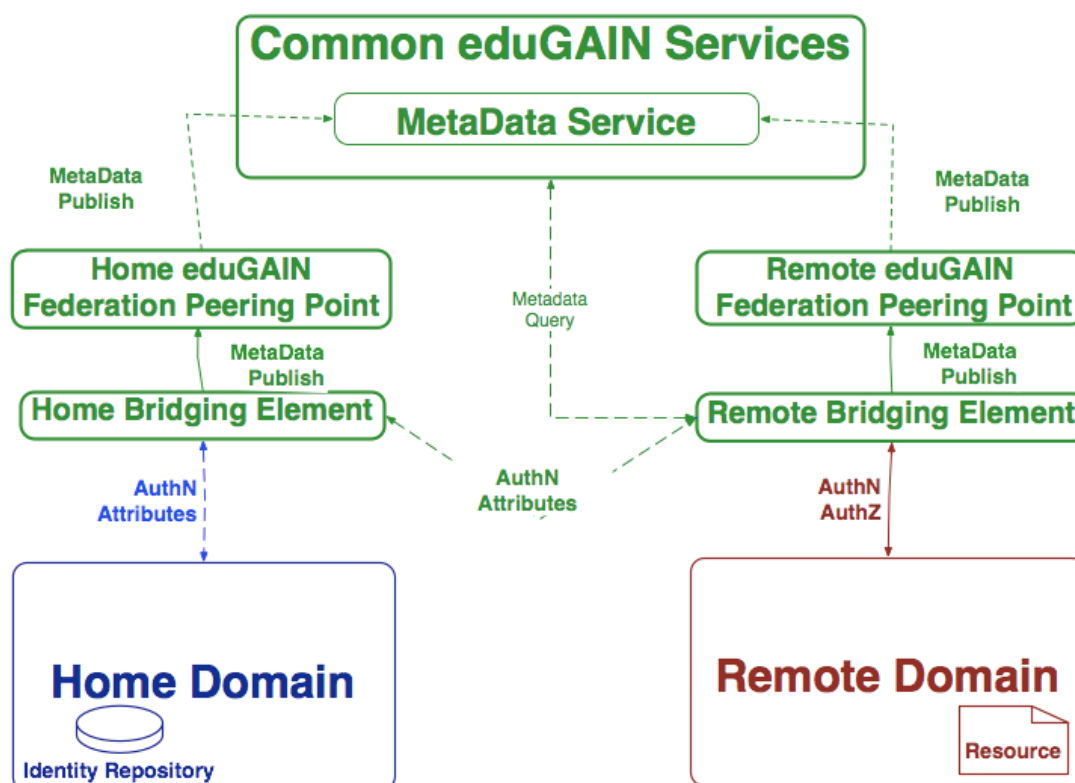


Figure 3.1: The eduGAIN architecture

Figure 3.1 is taken from deliverable DJ5.2.2bis GÉANT2 AAI Architecture and Design (the first version of the deliverable is [AAlarch]). The Home and Remote Bridging Elements link non-eduGAIN components into eduGAIN. The GIdP represents the interim Identity Repository for the GIdP users until their real Home Domain gets connected to eduGAIN.

The Figure 3.2 below is an example of how eduGAIN can be applied to GÉANT services (specifically, perfSONAR). When the user accesses a perfSONAR Resource (dotted line), the authorization is asked, through the R-BE and the H-BE (that are eduGAIN components), to the IdP of the Home Domain of the user (GIdP is just a particular instance of an IdP). eduGAIN thus “sits” in between the resources and the identity repositories of users wanting to access the resources. The MDS is an eduGAIN central service helping the R-BE to locate the home domain of the user. The MDS centralizes this location information received from Federation Peering Points (FPPs).

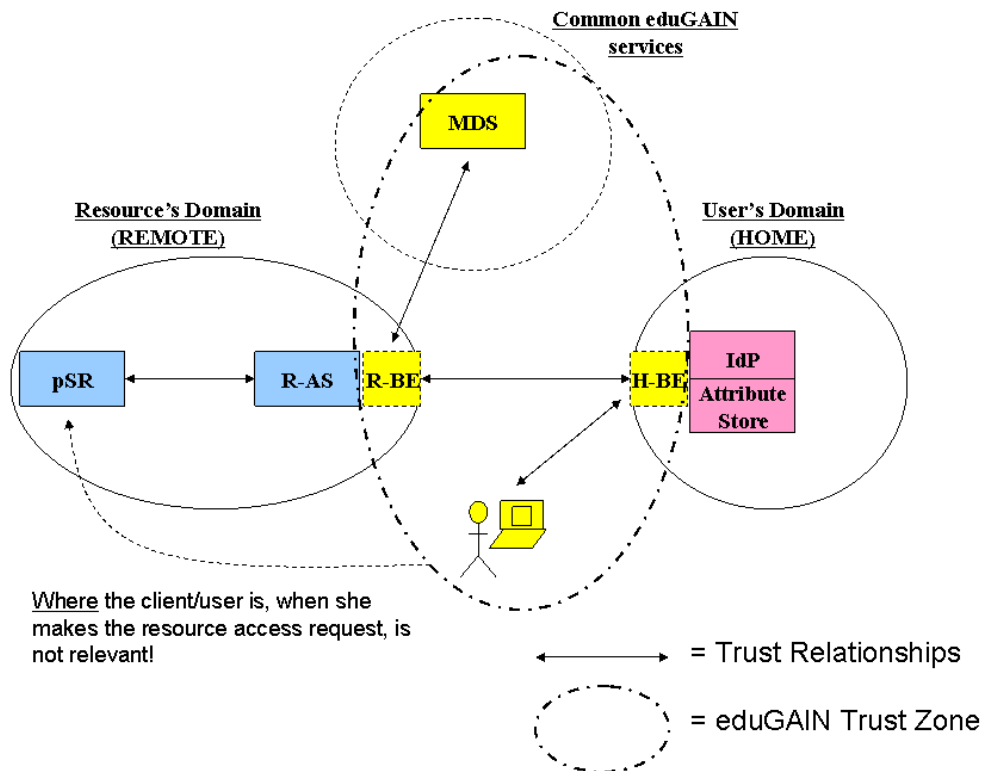


Figure 3.2: An example of eduGAIN usage to provide AA to perfSONAR resources

### 3.2 The GIdP Architecture

GIdP is a special eduGAIN Identity Provider (IdP) as shown in Figure 3.2 enhanced with an additional web browser accessible management tool. The components required are depicted in Figure 3.3.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

It was decided to make use of Shibboleth [Shibboleth] as the AAI technology for supporting the GIdP. The matching Shibboleth Bridging Element (BE) will allow integration of GIdP and any other Shibboleth-based AAI domains into the eduGAIN federation<sup>4</sup>. An eduGAIN Federation Peering Point (FPP) is needed as well, it is responsible for publishing the metadata to the eduGAIN Meta Data Service (MDS) required to interoperate within eduGAIN.

Since Shibboleth itself does not include an Authentication System, CAS [CAS] was chosen as the local Web-SSO system. OpenLDAP will be used as backend LDAP database for CAS as well as for the Shibboleth Attribute Authority. The latter is the entity deciding which attributes to retrieve from the database and to provide to the resources requesting information.

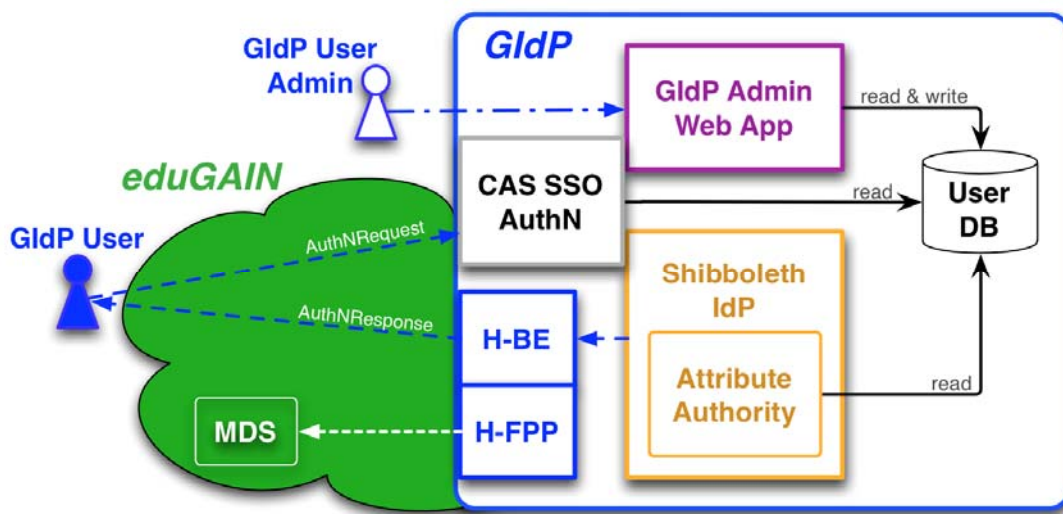


Figure 3.3: The GIdP architecture

In Figure 3.3, the GIdP user administrator connects to the GIdP directly via the Internet, without using eduGAIN for authentication: the authentication of the administrators is done locally in the GIdP with a local username and password file. Later on, this can be evolved making the GIdP itself a protected resource, and authenticating the GIdP administrators as “ordinary” users of a resource, which simply happens to be the GIdP itself. The GIdP user trying to access an eduGAIN protected resource (not part of this figure) gets redirected within his web browser to the GIdP authentication page provided by CAS. After successful authentication, the GIdP user gets first redirected to the Home Bridging Element (H-BE) and from there back to the eduGAIN protected resource we wanted to access in the first place. The H-FPP to MDS arrow simply represents the location data that is published from the H-FPP to the MDS beforehand.

The roles of persons involved with the GIdP are

<sup>4</sup> Other technology specific Bridging elements allow integration of other AAI technologies, like PAPI, A-Select, FEIDE

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

- GIdP service administrator
  - He has the power to manage the accounts of GIdP user administrators. In addition, he can delegate his rights to further GIdP service administrators. At least initially, staff from DANTE will take up the role of GIdP service administrator.
  
- GIdP user administrator
  - He is responsible to manage the digital identities of the GIdP users from the constituency of his NREN. In addition, he can delegate the rights he owns to another GIdP user administrator from the same NREN. (See 3.4)
  
- GIdP user
  - The digital identity provided by an NREN level AAI integrated with eduGAIN is not available yet, so he needs his GIdP user account to get access to eduGAIN protected resources.

The GIdP service administrators and the GIdP user administrators will use the GIdP administrator web application.

GIdP users will only need limited access to the GIdP administrator web application, primarily to change their password and review their set of attribute values.

### 3.2.1 The Delegation Model for the GIdP Administrators

The delegation model for the GIdP administrators (both service and user administrator) should be kept very simple:

- 1) User administrators have the right to create-modify-delete users belonging to their constituency (NRENs and connected institutions)
- 2) Service administrators have the right to create-modify-delete users administrator, and to suspend user or user administrator accounts in case of emergency
- 3) There is no hierarchy in the delegation model.
- 4) An administrator who has certain administration rights is responsible for delegating these rights only to further administrators entitled to get them and who know the procedures and duties to follow.
- 5) An administrator who gets rights delegated will be as powerful as the administrator who delegated them. All administrators, having equal administration rights are equal, there is nothing like one of them being a master administrator.
- 6) An administrator owning a certain right is entitled to revoke this right from other administrators who own it as well. The last remaining administrator owning a certain right cannot revoke his own right in order to prevent orphaned GIdP user entries. That is the opposite of rule 2) above.
- 7) Delegation and revoking of a certain right MUST be notified by e-mail to the administrator receiving or losing the right.

### 3.3 The Role of the GIdP User Administrator Managing GIdP User Entries

A GIdP user administrator is related to an NREN. He can add, modify or delete a GIdP user account, provided the user belongs to the constituency of the NREN the GIdP user administrator is affiliated with.

The GIdP user administrator does most probably not know much about these users himself, but he can rely on established relationships with the users' home institutions, which are customers of the NREN. A participating NREN has to define the rules on how to assure the correctness of the attribute values to be stored in an entry for a GIdP user belonging to its constituency. The GIdP user administrators **MUST** follow the rules defined by its NREN. This results in a process with reasonable assurance level and rather low administrative and technical overhead, provided the maximum number of users per GIdP user administrator is in the order of fifty.

With such an approach, the quality of data for the GIdP user entries can be controlled pretty well. It is not as good as a real home institution could achieve, but the GIdP user administrator, being affiliated to an NREN, is organizationally close to the home institution. The choice of having GIdP user administrators at the NREN level was justified at the beginning of 2.1.

On request of the resource owner, the GIdP user administrator should add, modify or remove in some GIdP user entries a resource specific attribute value related to a resource owned by the requestor. That enables a resource owner to authorize access to his resource based on the presence of a certain value in a resource specific attribute he receives (mapped to the eduPersonEntitlement described in 2.2.6), ignoring (or overriding) the other more general attributes (i.e. those described in 2.2.2, 2.2.3, 2.2.4 and 2.2.5).

Resource owners who want to request the addition of resource specific attribute values to GIdP user entries have in advance to register with the GIdP service administrator. At that time, a unique prefix gets assigned to the resource of that owner, which **MUST** be used for all resource specific attribute values specific for that resource.

The GIdP service administrators have only to deal with a low number of GIdP user administrators, and they are related to the NRENs with whom DANTE is already well related.

### 3.4 GIdP Administrator Web Application

The GIdP administrator web application must assist as much as possible the service and user administrators in the enforcement of GIdP rules (as defined in chapter 4) and restrictions on attributes and attribute values (as defined in the requirements in chapter 2.2). That is important, primarily for building trust in the digital identities the GIdP provides. Furthermore, the GIdP web application has to assure the uniqueness of the digital user IDs assigned by the many GIdP user administrators. It is also responsible to guarantee for attribute values, whose uniqueness has to be assured according to the eduGAIN policy (to be written and agreed upon), and for which reuse of values is prohibited beyond the lifetime of the individual entries.

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

### 3.4.1 Basic Features

The GIdP administrator web application

- MUST allow GIdP service administrators to
  - add, modify and delete a GIdP service administrator account,
  - add, modify and delete the accounts for GIdP user administrators,
  - reset the passwords for the GIdP user administrators,
  - delegate the own rights to further GIdP service administrators,
- MUST allow GIdP user administrators to the following actions for the GIdP users and administrators originating from the constituency of the NREN the GIdP user administrator is affiliated with,
  - add accounts
  - modify or delete accounts
  - reset the passwords
  - add, modify or delete resource specific attribute values
  - add or delete another GIdP user administrator account
  - delegate the own rights to another GIdP user administrator,
- MUST allow a GIdP users to
  - modify their own password,
  - see which attribute values are set for himself,
  - see who his GIdP user administrators are, so that they can be contacted for requests to change the registered attribute values
- SHOULD accept requests on a web form for adding a GIdP user. The request itself ends up in a queue for one of the corresponding GIdP user administrators. These GIdP user administrators get an alert by e-mail that they can check, complete and approve a new request. In the absence of such a web form, GIdP user administrators need to be notified offline, by some other methods, of the request to register a user.
- MUST store the data in the user database,
- MUST enforce password change on first authentication using a previously automatically generated password,
- MUST enforce the use of 'good' passwords, i.e. NOT allow users to choose 'weak' passwords.

### 3.4.2 Extended Features

The GIdP administrator web application

Project:	GN2
Deliverable Number:	DS3.14.1
Date of Issue:	09/03/07
EC Contract No.:	511082
Document Code:	GN2-06-326v7

- MAY allow GIdP system and user administrators to bulk import new accounts based on CSV files. The exact format to use will be defined by the GIdP system administrators.
- SHOULD allow registered resource owners to request the addition or removal of resource specific attribute values for GIdP user entries. The GIdP administrator web application automatically queues such a request for approval from one of the authoritative GIdP user administrators.

In addition, the GIdP administrator web application could be configured as an eduGAIN enabled resource itself. If available, GIdP user administrators and service administrators could then use their own federated eduGAIN identity to be authenticated for the administrator tasks. That way, it would even be possible that a GIdP user administrator would use a GIdP identity provided to him by the GIdP service provider. Since it does complicate the set-up, this feature is not recommended to implement during the initial phase of the project.

### 3.5 Migrating Users from the GIdP to their Institutional IdP

Since a user shall only have a GIdP user account as long as his home institution is not eduGAIN enabled, one has to think about how users might be migrated from the GIdP to their institutional IdP at a later stage. Unfortunately, a seamless migration as one would prefer, i.e. without involving neither the user nor the resource owners, seems unfeasible for “personalized resources”, i.e. resources locally storing user settings and permissions for users accessing the resource after the first login. The returning user’s identification is generally based on a unique identifier (see 2.2.5.1), and since this unique identifier changes during migration, a seamless and fully automatic migration is impossible.

## 4 GIdP Rules

The GIdP rules have to be in compliance with the upcoming eduGAIN policy; at least its minimal requirements must all be met in order to become part of eduGAIN.

The eduGAIN policy will have to cover the

- minimal level of assurance required for eduGAIN identities,
- minimal set of attributes to be able to be provided by eduGAIN IdPs, most probably based on the SCHAC specs,
- requirements for metadata availability.

### 4.1 GIdP Usage

A user **MUST** be entitled to get a GIdP user account provided:

- the IdP of his home institution is not eduGAIN enabled<sup>5</sup>,
- he originates from a constituency of an NREN,
- he has the professional requirement to access one or more eduGAIN enabled resources.

A GIdP user administrator **MUST** be affiliated to a NREN on which behalf he manages GIdP user accounts.

A GIdP user administrator **MUST** have a GIdP user administrator account as long as he has to manage GIdP user accounts.

---

<sup>5</sup> Although exceptions are acceptable, i.e. for early adopters of GÉANT services whose institution is already connected to eduGAIN but without all the registration procedures already in place.

## 4.2 Obligations

### 4.2.1 GIdP Service Provider (DANTE)

- Guaranteed GIdP service availability
  - The authentication service for the GIdP users SHOULD have an availability high enough not to reduce the overall availability of the services it will support (for their AA needs). The service must be available 24/7 with the GIdP service administrator (or their backups) providing support during normal working days and hours.
  - The GIdP administrator web application can have a somewhat lower availability, since it affects primarily the GIdP user administrators and not all GIdP users in their daily business. However, this availability should be compatible with potentially critical operations such as suspending a user account.
- Verification of the identity of the GIdP service administrators.
- Enforcement of the GIdP rules
  - The GIdP administrator web application must assist as much as possible the service and user administrators in the enforcement of GIdP rules.
- GIdP compliance with eduGAIN policy
  - Operate the GIdP service in compliance with the upcoming eduGAIN policy.

### 4.2.2 GIdP Service Administrators

The GIdP service administrators are responsible to

- verify the identity of each GIdP user administrator,
- instruct the GIdP user administrators appropriately, and take appropriate actions if/when it is realised that some user administrator didn't correctly enforce GIdP policies. An example would be asking a GIdP user administrator to investigate cases of resource misuse originating from registered users, and/or suspend the validity of user and/or user administrator accounts until the investigation is completed.
- revoke GIdP user administrator accounts whenever no longer required.

### 4.2.3 GIdP User Administrators

The GIdP user administrators are responsible to

- guarantee the required assurance of identity for the individuals requesting a GIdP digital identity.

- provide minimal support to their user base from the constituency of their NREN, e.g. support for lost password and for questions regarding the supplied attributes.
- properly check the correctness of the attribute values stored for the GIdP users,
- verify that a resource owner requesting the addition, modification or removal of a resource specific attribute is entitled to do so,
- revoke GIdP user accounts whenever no longer required, or as a consequence of resource misuse.

The GIdP user administrators (or their backups) should be contactable by the GIdP users or by the GIdP service administrator during normal working days and hours

## 5 Software to Use

### 5.1 IdP Component

- Latest Shibboleth 1.3 IdP. To be upgraded to Shibboleth 2.0 when available.
- eduGAIN Shibboleth Bridging Element
- eduGAIN FPP
- OpenLDAP database
- CAS Web-SSO package

### 5.2 GIdP Administrator Web Application

- PHP, JSP or another web app language
- SWITCHaai VHO administrator tool (open source, written in PHP)
  - This software was developed by SWITCH for a similar purpose, however, the model of operation is different from the eduGAIN GIdP. Nevertheless, it can be used as a starting ground to implement the features required for the eduGAIN GIdP. DANTE will first check out this code to find out what to reuse and what to write from scratch.

## 6 Hardware Needs

### 6.1 Basic Hardware to Start with

Two Linux servers with redundant disks and power supply. One for production, the other for tests and version upgrades and as possible fallback machine in worst-case scenarios.

### 6.2 Extended Hardware for full Service

Three Linux servers with redundant disks and power supply. Two for production, one for service and the other one hot stand-by. The third server is for tests and version upgrades.

## 7 Dependencies & Next Steps

The GIdP has the following external dependencies:

- the eduGAIN bridging element for Shibboleth,
- the eduGAIN FPP,
- the eduGAIN policy document to know the minimum requirements the GIdP has to fulfil,
- the eduGAIN attribute specification to know which minimal set of attributes has to be provided. In the interim the attribute set defined in 2.2 will be supported,

## 8 Conclusions

The document presented the motivation, detailed design and policy of the GIdP, an interim Identity Provider service meant to ease the adoption of the eduGAIN Authentication and Authorization framework. In the long term, the institutional Identity Providers should be all connected to eduGAIN and provide identification and attributes for the users of GÉANT services, and GIdP should gradually disappear. However, the experience gained during the development and the deployment of GIdP will be exploited to ease this wide adoption of eduGAIN.

The main design highlights of the GIdP are:

- 1) the definition of an attribute set (for the users registered in GIdP) after the requirements collected from some of the GN2 activities developing services wanting to adopt the eduGAIN AAI framework. A major requirement was to include attributes describing the projects (if any) a user is working on, along with project-specific roles
- 2) the definition of a simple responsibility hierarchy for the registration of GIdP users: at least one GIdP user administrator per NREN is responsible for registering users of the NREN or of institutions connected to the NREN wanting to use GN2 services. A single GIdP service administrator is responsible for registering the GIdP user administrators

The immediate next step of the GIdP activity, along with the development and deployment of the necessary software, will thus be, together with all the NRENs, the identification of the responsible GIdP user administrators.

## 9 References

- [CAS] Central Authentication Service - Single Sign-on for the Web  
<http://www.ja-sig.org/products/cas/>
- [eduPerson] <http://www.educause.edu/eduperson/>
- [SA3-Wiki] <http://wiki.geant2.net/bin/view/SA3/Sa3GidpMain>
- [SCHAC] <http://www.terena.org/activities/tf-emc2/schac.html>
- [Shibboleth] <http://shibboleth.internet2.edu/>
- [VHO] SWITCHaai Virtual Home Organization  
<http://switch.ch/aai/vho/>
- [AAIarch] **DJ5.2.2 GÉANT2 AAI architecture and design**
- [AAIarchbis] **DJ5.2.2 bis GÉANT2 AAI architecture and design:**  
**<http://www.rediris.es/jra5wiki/index.php/Architecture%20document>**

## 10 Acronyms

<b>AA</b>	Authentication and Authorisation
<b>AAI</b>	Authentication and Authorisation Infrastructure
<b>BE</b>	Bridging Element (eduGAIN)
<b>CAS</b>	Central Authentication Service (a software package for local Web-SSO)
<b>CSV</b>	Comma Separated Values
<b>FPP</b>	Federation Peering Point (eduGAIN)
<b>GIdP</b>	GÉANT Identity Provider
<b>IdP</b>	Identity Provider
<b>MDS</b>	MetaData Service (eduGAIN)
<b>SCHAC</b>	SCHema for ACademia (TERENA TF-EMC2)
<b>SSO</b>	Single Sign-on
<b>VHO</b>	Virtual Home Organisation (SWITCHaai)