

20.03.08

Deliverable DS3.14.6: GÉANT Identity Provider (GIdP) Operational Procedures



Deliverable DS3.14.6

Contractual Date: 29/02/08
Actual Date: 20/03/08
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: SA3
Work Item: WI14
Nature of Deliverable: R – Report
Dissemination Level: PU – Public
Lead Partner: DANTE
Document Code: GN2-08-052v2

Authors: Toby Rodwell (DANTE), Maurizio Molina (DANTE), Ian Thomson (DANTE)

Abstract

This document describes the resources involved in GÉANT Identity Provider (GIdP) administration and support. It describes the roles, responsibilities and interactions of all personnel involved, and also gives details of the effort required.

Table of Contents

0	Executive Summary	iv
1	GIdP overview	1
2	GIdP service overview	3
	2.1 Users of the GIdP service	4
3	GIdP roles and functions	5
	3.1 GIdP User Administrator	6
	3.1.1 Role description	6
	3.1.2 Effort	7
	3.2 GIdP Service Administrator	7
	3.2.1 Role description	7
	3.2.2 Effort	9
	3.3 GIdP System Administrator	9
	3.3.1 Role description	9
	3.3.2 Effort	10
	3.4 Incident Management	10
	3.4.1 Role description	10
	3.4.2 Effort	10
	3.5 Problem Management	11
4	Effort summary	12
5	Communication flows	14
	5.1 User Admin registration by Service Admin	14
	5.2 Peer User Admin registration	14
	5.3 End user registration	14
	5.4 User signalling a problem to UA	15
	5.5 UA (or other application service desk) escalating a GIdP user problem to Incident Management	15
	5.6 User signalling a GIdP problem directly to Incident Management	16
	5.7 UA signalling a GIdP WI problem to Incident Management	16
	5.8 ServA signalling a GIdP WI problem to Incident Management	16

6	Conclusions	17
7	References	18
8	Acronyms	19

Table of Figures

Figure 1.1: GIdP architectural view	2
Figure 2.1: GIdP service view	3
Figure 3.1: Roles and functions involved in the GIdP service delivery	6
Figure 3.2: Example configuration of LDAP JXplorer to connect as an administrator to the GIdP LDAP directory.	8

0 Executive Summary

GÉANT2 services such as perfSONAR [6] and autoBAHN [7] provide access to sensitive network data or resources, and therefore demand secure authentication and authorisation. The eduGAIN initiative and framework [5] was initiated to provide secure access to any GÉANT2 service. However, in the short term not all national federations will be able to deploy, test and roll-out all the components needed to connect to eduGAIN. Therefore GÉANT Identity Provider (GIdP) was created to provide an interim secure authentication and authorisation solution. For a description of GIdP aims and services (including levels of service), see [1].

This Deliverable describes the operational procedures and human resources involved in GIdP administration and support, including roles, responsibilities and interactions. It assumes a background knowledge of eduGAIN [5] and the aims and services of GIdP [1].

The roles and responsibilities are:

- GIdP System Administrator, responsible for the installation of the software needed to deliver the service on the GIdP servers (primary and backup), and for the “health check” of those servers.
- Several GIdP User Administrators (at least one per NREN using the GIdP service), responsible for registering and managing end GIdP users.
- GIdP Service Administrator, responsible for registering and managing GIdP User Administrators.
- Incident Management (L1 support) within the GN2 Service Desk, acting as the single point of contact for the GIdP User Administrators and the end GIdP users.
- Problem Management (L3 support), handled by developers/maintainers of Software used by GIdP.

The amount of effort required to deliver the GIdP service is estimated at:

- 0.25 Person Months (PM) per User Administrator.
- 0.1 Full-Time Equivalent (FTE) for the GIdP Service Administrator.
- 0.1FTE for the GIdP System Administrator (plus approximately one week to install each GIdP instance).
- 0.2 FTE (plus 2 PM initial document writing) for the Incident Management support.
- 0.3 FTE for Problem Management (L3 support).

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

1 GIdP overview

GÉANT2 services such as perfSONAR and autoBAHN provide access to sensitive network data or resources, and therefore demand secure authentication and authorisation. To grant access without replicating user accounts on each service or resource, several NRENs have deployed their own national Authentication and Authorization Infrastructure (AAI). However, the communication between these infrastructures is often restricted by incompatible technologies and by limited mutual trust.

To overcome this severe limitation, GN2 began the eduGAIN initiative and framework [5]. eduGAIN is a confederation of national AAI federations, and ultimately every user belonging to a federation connected to eduGAIN will be able to access any GÉANT2 service through it.

However, in the short term not all national federations will be able to deploy, test and roll-out all the components needed to connect to eduGAIN. This interim situation is the reason for the production of GÉANT Identity Provider (GIdP). GIdP provides a “light-weight” interim identity repository that is connected to eduGAIN, and where early adopters of GÉANT2 services can have an account for accessing them. It is expected that GIdP will become obsolete when the eduGAIN interconnection is fully rolled-out in all national AAIs.

The GIdP architecture is summarised in Figure 1.1 below. There are three important concepts:

- The core data GIdP stores are user identities and related attributes. These are contained in a LDAP directory.
- When users try to access GÉANT2 services protected by eduGAIN and get redirected to GIdP for authentication, software translates the Authentication requests from eduGAIN primitives into queries understood by the LDAP directory and then translates and replies back into eduGAIN compliant responses.
- Authentication queries and Access grant/deny decisions traverse the eduGAIN infrastructure. In particular, they pass through two Bridging Elements (H-BE and R-BE) that translate messages back and forth from the AAI federation the service belongs to and the AAI federation the user belongs to. This translation allows different national level AAI federations (possibly based on different technologies) to work together, and is one of the key benefits of eduGAIN.

This document describes the roles and responsibilities of the human resources supporting the GIdP service, or benefiting from it. It assumes a background knowledge of eduGAIN and GIdP. For further details of eduGAIN, please refer to [5]. For details of GIdP architecture and service, please refer to [1].

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

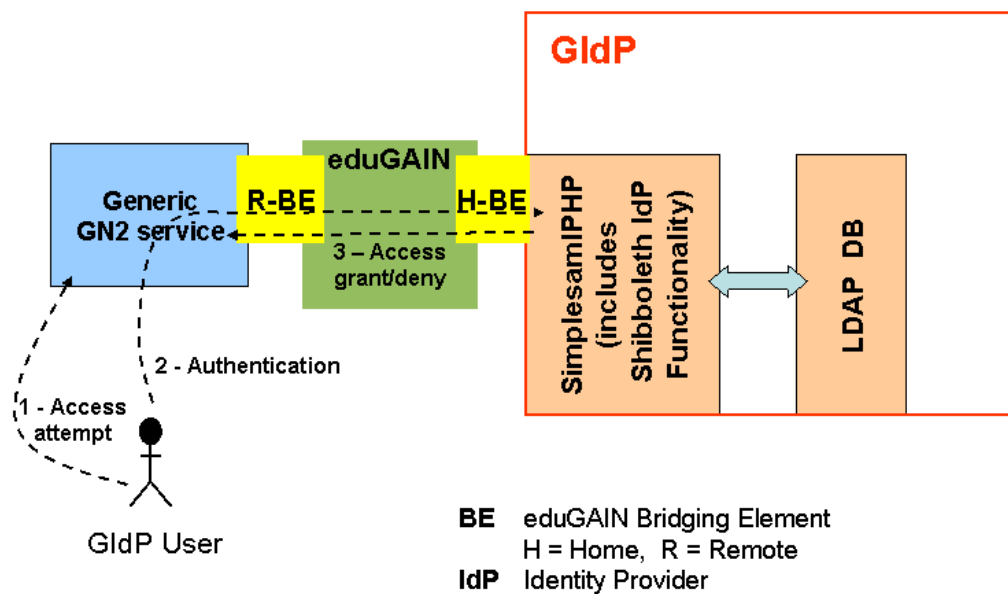


Figure 1.1: GIdP architectural view

2 GIdP service overview

The GIdP service consists of:

- An Authentication and Authorisation service, triggered by users when they try to access GÉANT2 services protected by eduGAIN (as described above).
- A GIdP identity repository administration service, which stores the AAI information (in the LDAP directory) through a Web Interface (WI). This GIdP Web Interface was developed in DANTE and documented in [2].

Figure 2.1 summarises these services:

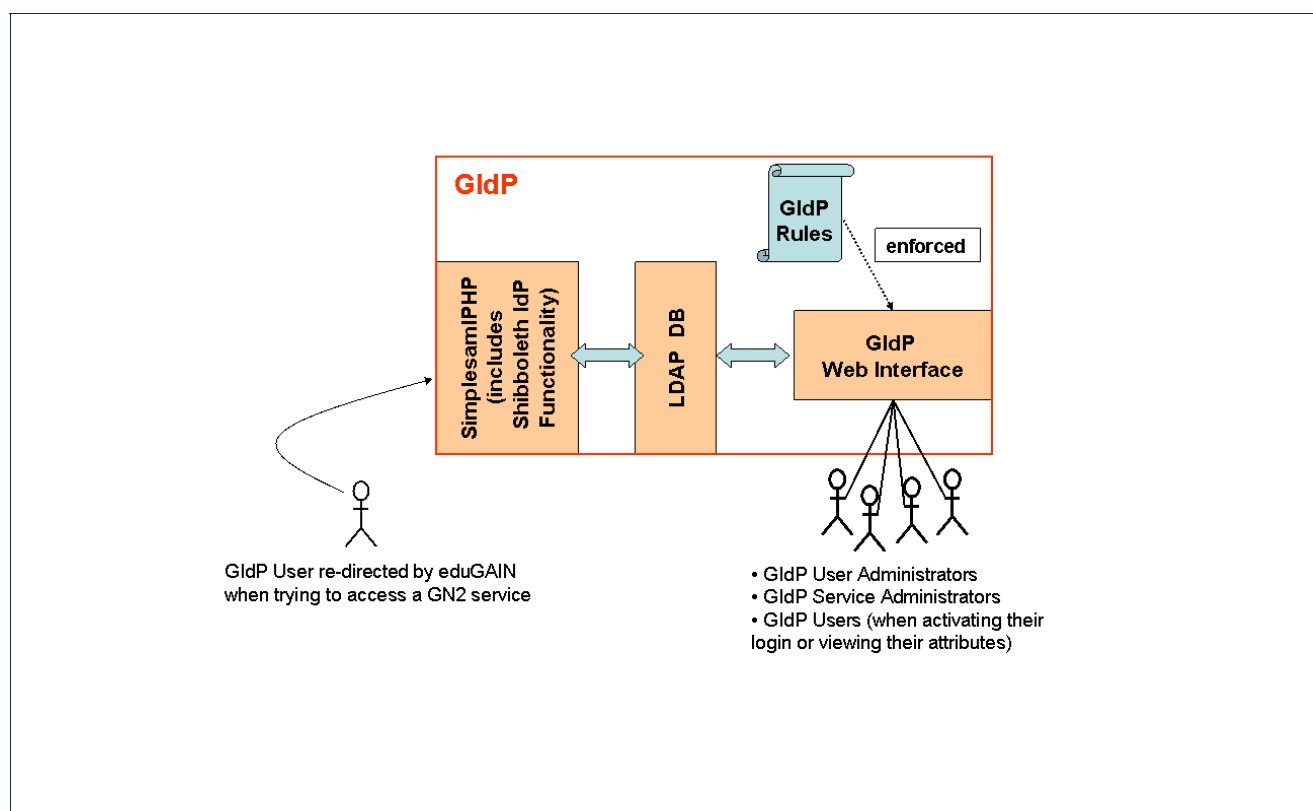


Figure 2.1: GIdP service view

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

2.1 Users of the GIdP service

The basic users of the GIdP Authentication and Authorisation service are individuals belonging to an NREN or its connected institutions (NREN “constituency”) that get their identity registered in the GIdP LDAP directory, and with that can access GÉANT2 services protected by eduGAIN. These users are referred to as GIdP users.

GIdP users have to be registered, and this registration is done by the GIdP User Administrators (UA) of the users’ constituencies. The request for registration may come to the UA from the GIdP users themselves, or from the owners of eduGAIN protected resources, or be initiated by the GIdP UAs. The first set of GIdP Users are expected to be the participants of the perfSONAR pilot.

Other actors involved in the GIdP Authentication and Authorization service are GN2 Service Providers administrators (or “resource owners”) who rely on GIdP as a trusted repository of identities and the authenticator of users trying to access their resources through the mediation of the eduGAIN infrastructure. Because of GIdP, resource owners do not have to maintain dedicated accounts for these users. However, resource owners play a minimal role in the operation of GIdP, and they are not discussed any further in this document.

The GIdP User Administrators register GIdP users through the GIdP Web Interface, and are thus the primary customers of the GIdP identity repository administration service.

The identity of the GIdP User Administrators is registered in the same GIdP repository by a GIdP Service Administrator, who therefore also benefits from the GIdP identity repository administration service. Note that although the identity repository of the UA is the same LDAP directory used to store the GIdP users, the UA cannot access any eduGAIN protected resources with these credentials, and thus are *not* beneficiaries of the Authentication and Authorisation service.

Finally, end users must connect to the GIdP WI to activate their login before they can make use of the GIdP Authentication and Authorisation service, and can connect to the GIdP WI whenever they want to review their attributes (and possibly get in touch with their UA if they need to correct them). Therefore, GIdP users are also customers of the GIdP identity repository administration service.

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

3 GIdP roles and functions

The GIdP service is delivered as a joint effort of several roles, each of them having specific tasks. The GIdP Service Administrator (ServA) and GIdP User Administrators (UA) were described above. Note that there should be at least one UA (plus, optionally, one or more back-up UAs) per NREN using GIdP. At the time of writing, 23 NRENS have nominated a UA. The GIdP ServA is within the GN2 service desk function, while the UAs are part of the NRENS' staff.

The GIdP System Administrator (GIdP SysA) is responsible for the installation of the software needed to deliver the service on the GIdP servers (primary and backup), and for the health-check of those servers. The GIdP SysA role is part of the GN2 service desk function.

Then, since GIdP is a common component used to enable the delivery of other services (for example PerfSONAR and autoBAHN), an Incident Management service is provided for all users of GIdP services. Incidents may be reported by end users, application service desks of GN2 services, and GIdP UAs. Incident Management is managed within the GN2 service desk function

Finally, incidents that cannot be solved easily need to be escalated to Problem Management. Problem Management is handled by developers or maintainers of the code base used to support the GIdP service, who are either in DANTE Systems team or in NRENS (and, in the future, may be provided by an eduGAIN service activity).

Figure 3.1 summarises the several roles involved in the GIdP service delivery and their allocation to functions.

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

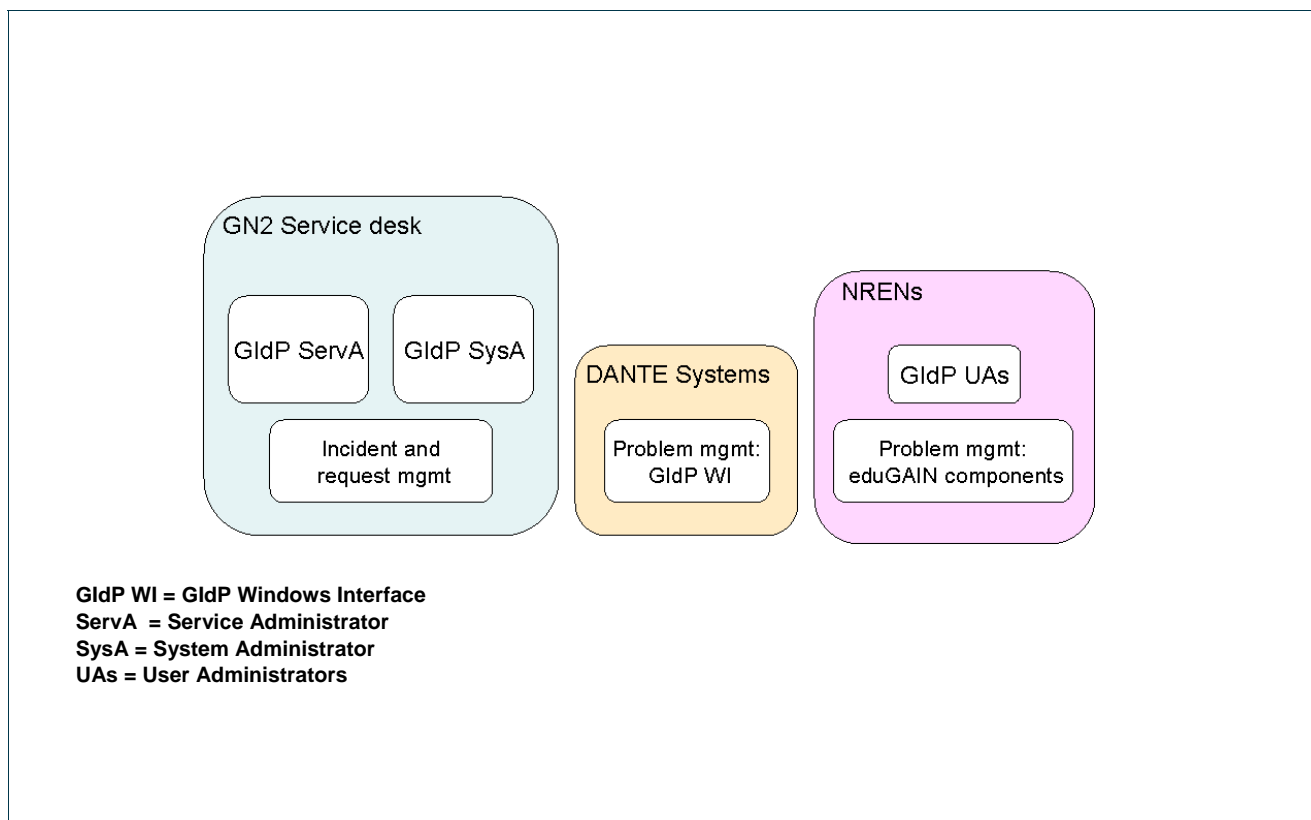


Figure 3.1: Roles and functions involved in the GIdP service delivery

The detailed responsibility of each of the listed roles is described in the sections that follow. Their associated communication flows are described in section 5.

3.1 GIdP User Administrator

3.1.1 Role description

User Administrators (UAs) are NREN staff, and are responsible for registering and managing the digital identities of the GIdP Users in their NREN constituency. In addition (for the purposes of load sharing or redundancy), they can create other UAs in their NRENs and delegate to them the same administrative rights they themselves have.

The GIdP UAs must:

- Verify the identity of individuals requesting a GIdP digital identity.
- Provide a basic level of support to their user base from the constituency of their NREN, for example help with lost passwords and for questions regarding the supplied attributes.

- Ensure the attribute values they register for the GIdP Users are valid.
- Verify that a resource owner requesting the addition, modification or removal of a resource specific attribute to some GIdP Users is entitled to do so (these resource-specific attributes are mapped to eduPersonEntitlement, see [2], section 2.2.6.1).
- Revoke or suspend GIdP User accounts when they are no longer required, or as a consequence of resource misuse.
- Should be contactable by the GIdP Users or by the GIdP ServA during normal working hours. Their contact details can be found on the GIdP WI login page, which GIdP Users have to visit to activate their account and to where they are redirected when they have to authenticate themselves to resources.

UAs perform their tasks exclusively through the GIdP Web Interface (GIdP WI), as described in the GIdP WI guide and self-paced training. Note that the GIdP WI limits the visibility of UAs to their constituency (that is they can see and manage the users and the UAs of their constituency, but they will not see who the GIdP Users of other constituencies are).

3.1.2 Effort

- A UA needs (approximately) two or three days to read the GIdP WI guide [2], follow the self-paced training [3] and start becoming familiar with the GIdP WI.
- It is then estimated that a UA spends no more than 20min for each user they register, assuming they have at hand the data they need to input. This time includes that needed to communicate credentials to the user, according to whatever confidentiality procedures they have in place. The maximum number of users per each constituency should be of the order of 50.

This gives a total effort of approximately five Person Days, or 0.25 PM.

3.2 GIdP Service Administrator

3.2.1 Role description

The GIdP Service Administrator (ServA) is required to:

- Create the accounts for the first UA of each NREN exploiting the GIdP service, verifying their identity (Note that once the initial UA is created for an NREN, it then becomes that person's responsibility to create additional UAs for their NREN, if that is what is required).
- Instruct the GIdP UAs, and take appropriate actions if/when it is realised that some UA did not correctly enforce GIdP policies. An example would be requesting a GIdP UA to investigate cases of resource misuse originating from registered users, and perhaps suspending user and/or UA accounts until that investigation is completed.
- Revoke GIdP UA accounts when they are no longer required.

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

The ServA creates and manages UA accounts through the GIdP WI.

The ServA is also able to access the GIdP WI logs for troubleshooting issues with UA or end User registration. Logs are available in the `.../tomcat/logs` directory of GIdP WI. Information logs are available in the `catalina.out` log file and debug logs are available in the `audit.log` file. Logs record the IDs of GIdP Users or GIdP UAs that have been created, modified, deleted, suspended, terminated or re-activated, along with the ID of the UA/ServA who performed the action. Logs also record details of all authentication attempts, successful or otherwise. Since the GIdP WI generates automatic e-mails for certain events, the logs also keep track of to whom these information e-mails are sent to.

The ServA requires the skills to directly create, modify or delete the LDAP directory of GIdP, through command line interface commands or through an LDAP explorer (like JXplorer, see Figure 3.2), though whenever possible this should be avoided and done through the GIdP WI.

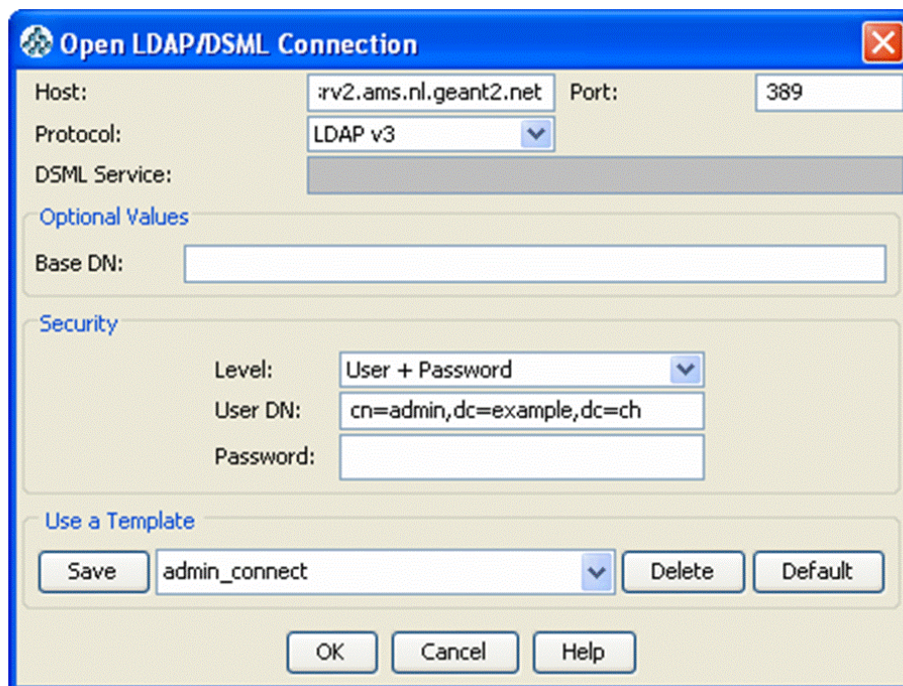


Figure 3.2: Example configuration of LDAP JXplorer to connect as an administrator to the GIdP LDAP directory.

Note: The above example should be done only in extreme cases, as any such intervention to the database might break dependencies created by the GIdP WI and thus prevent it working properly.

In conclusion, the GIdP ServA's responsibilities are limited to those aspects related to UA registration and management of the GIdP, and all these tasks should be achievable through the GIdP WI. Only in case of malfunction may it be necessary to access the LDAP directory directly (possibly, with the help of the GIdP System Administrator). The GIdP ServA needs to be aware of the GIdP policies, documented in [1].

Note that the GIdP ServA is not responsible for installing and troubleshooting the other components of GIdP that are necessary for delivering the user authentication and attribute assertions. This is responsibility of the GIdP System Administrator.

The GIdP Service Administrator is within the GN2 service desk function

3.2.2 Effort

- The GIdP ServA needs, roughly, one or two days to become familiar with the GIdP WI.
- For registering a UA, they need to spend no more than 20 minutes, assuming they already have the data they need to input. This time includes the time needed to communicate to the user their credentials, in accordance with the confidentiality procedures they have in place. The number of the UAs should be comparable to the number of the NREs (approximately 30).

Note that at the time of this writing, the identities of 23 UAs were already created in the GIdP test instance, and the resulting LDAP directory can be copied to the GIdP production instance without the need of repeating the registration process. The running effort for the GIdP ServA should be around 0.1 FTE

3.3 GIdP System Administrator

3.3.1 Role description

The GIdP System Administrator (GIdP SysA) is required to:

- Install all the software needed for GIdP (this includes the SimpleSAML software, the certificates signed by the eduGAIN CA, the LDAP, and the GIdP WI) on the GIdP primary (production) server, following the installation notes in [4].
- Repeat the procedure for the GIdP backup (production) server.
- Set up the periodic synchronization of the LDAP directories between the primary and backup servers.
- Ensure the availability and network connectivity of both servers.
- Detect any primary (production) server failures and accordingly change the appropriate DNS entry so as to direct all GIdP requests to the backup server.
- Update SW installations when those responsible for GIdP continued development (see 3.5) fix bugs or release new versions.
- Troubleshoot (possibly with the help of L3 (GIdP developer) problems related to the GIdP SW, the GIdP WI and GIdP LDAP directory, possibly with direct access through a LDAP explorer (Figure 3.2) or through LDAP CLI commands.

Note that the GIdP SysA is not responsible for the initial installation of the OS on the servers, nor for their patching. This is a task for the nominated GÉANT2 systems administrators.

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

The GIdP SysA is part of the GN2 service desk and, being aware of the GIdP software configuration details, provides L2 support. The GIdP SysA decides jointly with Incident Management if and when to escalate a problem to the developers who provide L3 support.

3.3.2 Effort

- Maximum one week of effort should be estimated for the installation of all the prerequisite SW and of the GIdP WI for the first server (presumably less for the second server).
- The other tasks after the initial installation should not take more than 0.1 FTE.

3.4 Incident Management

3.4.1 Role description

Incident Management is part of the GN2 service desk function and should provide a single point of contact for all GIdP users (UAs and GIdP users reporting problems they think are related to GIdP), and for other application service desks.

Its responsibilities are:

- Deal with user's signalled incidents.
- Try to troubleshoot them with the aid of a (limited) knowledge base (L1 support).
- Maintain and update a knowledge base.
- Maintain a FAQ that should eventually be accessible from the GIdP login page¹.
- Maintain statistics of problems signalled, solved, escalated, etc.
- If incidents cannot be solved, consult the GIdP ServA and/or the GIdP System Administrator (representing L2 Support), and if a solution can't still be found, decide if to escalate it to Problem Management.

3.4.2 Effort

The estimated effort for the Incident Management support in the GN2 service desk is 0.2 FTE, plus 2 MM for the detailed definition of the needed procedures. These detailed procedures are not described in this document, but will be part of an operational document developed jointly by the GN2 service desk and the GIdP designers/developers.

¹ This feature is not currently part of the GIdP WI, but only requires the addition of a static link to the GIdP WI.

3.5 Problem Management

Problem Management is provided by two developer groups; one for GIdP WI (in DANTE), and one for all the remaining SW composing GIdP. Most of this software was developed by NREN staff within JRA5. If there is to be an eduGAIN support activity, JRA5 would provide the obvious source of resource.

The role of Problem Management support will be bug fixing and the implementation of additional features in GIdP WI resulting from UA feedback. It can thus be viewed as L3 support.

The estimated effort for Problem Management is around 0.3 FTE (0.15 FTE for the GIdP WI and 0.15 FTE for the other components). A maximum of 1 MM of short term effort is estimated to redesign and implement some parts of the GIdP WI.

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

4 Effort summary

The following table summarises the effort for providing the GIdP service. Note: this assumes that the GIdP software is used “as it is” at the time of writing, and that no formal Release Management is carried out.

Note also that the communication flows among roles has been described as it exists at the time of the writing. Refinements to these procedures and their documentation (mainly for internal use by the GN2 Service Desk) are expected to happen in the next two months, as a joint effort by the GN2 Service Desk and the SA3 WI14 leader. This effort is accounted for as the 2MM one off effort for "Incident Management (L1 support)" described in the table below. Note that these are estimated figures only.

Role	Where (function)	One-off effort	Steady Effort
GIdP UA	At least one in each NREN using GIdP	2-3 days for familiarising with the GIdP WI 20 min. for each user they register	Unestimated
GIdP ServA	In GN2 service desk	Account creation and password communication for 23 UA has already happened, so the residual one off effort should be low (< 1 week)	0.1 FTE
GIdP System Administrator (L2 support)	In GN2 service desk	< 1 week for the first production GIdP server. Hopefully less for the second one	0.1 FTE
Incident Management (L1)	In GN2 service desk	2 MM	0.2 FTE

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

support)			
Problem Management (L3 support)	In DANTE for GIdP WI, in eduGAIN Service Activity or in NRENs for the remaining SW	1MM	0.15 + 0.15 FTE
Total effort (outside DANTE)		~4MM (UA)	0.15 FTE + UA effort
Total effort (DANTE)		~ 3.5 MM	0.5-0.6 FTE

Table 4-1 GIdP operation effort summary

5 Communication flows

5.1 User Admin registration by Service Admin

Roles involved: One User Administrator (UA), the Service Administrator (ServA).

Description: A UA is nominated as the initial GIdP UA for an NREN (cases of “self nomination” are also possible) and the ServA is notified about this nomination (communication method is not specified). The ServA checks that this person is entitled to take this role, and if so creates an account for the nominee using the GIdP WI. The credentials are sent through encrypted mail (preferably) or over the phone. The ServA must ensure that the UA has received the appropriate documentation about GIdP-WI (manual and self-paced training)². The UA contact information and the public PGP key (if used) must be stored by the Service Admin securely.³

5.2 Peer User Admin registration

Role involved: Two UAs in the same constituency.

Description: A UA creates an account for a peer user admin in the same NREN and communicates to them the access credentials using any security mechanisms they have in place. The UA creating the account must ensure that the UA created has received the appropriate documentation about GIdP-WI (manual and self-paced training). Note: the ServA receives an automatic e-mail notification about the creation but does not need to take any action.

5.3 End user registration

Roles involved: One UA, one GIdP user in the same constituency.

² At the time of writing, 23 UAs have already been nominated, with the SA3 WI14 leader having acted as a “temporary” ServA. All the UAs have received the manual, but not the self-paced training.

³ Currently this information is partly on the GIdP wiki and partly in the possession of the SA3 WI14 leader. This information will be handed over to the ServA

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

Description: A UA is notified (communication method not specified) about the need to create a user account for a user in their NREN constituency. The UA checks that this person is entitled to receive such an account and that the personal details registered are correct. Also, if any resource specific attributes for the user are registered, they must ensure that the user is entitled to have these (resource-specific attributes are mapped to eduPersonEntitlement, see [2], section 2.2.6.1). This may require interaction with resource owners. The UA then creates an account for the user through the GIdP WI and communicates to her/him the access credentials using any security mechanisms they have in place in the NREN constituency. The UA creating the account must only ensure that the end user receives the link to the GIdP-WI where to activate the login.

5.4 User signalling a problem to UA

Roles involved: End GIdP User, UA.

Description: A User contacts one of the UA of his constituency about a problem (typically, this will be a problem in either the user account on the GIdP WI itself or about the fact that the user cannot get access to a resource through GIdP authentication). If the UA understands that this problem can be solved using the GIdP WI (for example, a simple password reset, or a modification in the user's attributes), they can fix the problem, and inform the user. Incident Management support doesn't need to be informed, unless beneficial for any reason. If not, see 5.5.

5.5 UA (or other application service desk) escalating a GIdP user problem to Incident Management

Roles involved: End GIdP User, UA or application service desk, Incident Management, <GIdP SysA>⁴, <Problem Management>.

This is the continuation of the previous flow: If the UA does not understand the problem or determines that it requires action on the GIdP internals, she/he must inform Incident Management in the GN2 service desk (L1 support). L1 support must handle the problem, possibly escalating it to GIdP SysA (L2 support) and Problem Management (L3 support), and ultimately communicating it back to the UA (the latter having the responsibility to get in touch with the end user who raised the problem).

The role contacting the GN2 service desk can also be another application service desk, having been contacted by a user of that application. The flow is identical as the one just described with the "application service desk" replacing the "UA"

⁴ < > Brackets indicate that this role's presence in this flow may or may not be necessary

5.6 User signalling a GIdP problem directly to Incident Management

Note: This case is described to allow users to report incidents without contacting their UA first.

Roles involved: End GIdP User, Incident Management, <UA>, <GIdP SysA>, <problem Management>.

Description: A User contacts the Incident Management (L1 support) in the GN2 service desk about a problem (typically, this will be a problem in either the user account on the GIdP WI itself or about the fact that the user cannot get access to a resource using GIdP authentication). If the L1 support understands it is a problem related to the user's attributes only, they must inform the UA of the user's constituency and ask them to take charge of the problem (the end user must also be informed of this "redirection"). If L1 support understands that this problem has to do with the GIdP internals, they must solve the problem, possibly with the help of GIdP SysA (L2 support) and Problem Management (L3 support), and get back in touch with the end User after the problem is solved. The UA of the same NREN constituency of the end user having signalled the problem doesn't need to be informed, unless this is beneficial for any reason.

If a problem is signalled to the L1 support by a third party (for example, an application service desk), they must take care of the problem as before, except that the responsibility of informing an end GIdP user or a UA about the problem solution falls onto the signalling party.

5.7 UA signalling a GIdP WI problem to Incident Management

Roles involved: GIdP UA, Incident Management, <GIdP Service Administrator>, <GIdP SysA>, <problem Management>.

Description: A UA contacts the Incident Management (L1 support) in the GN2 service desk for a problem with their usage of the GIdP-WI. The L1 support should determine if it is a problem related to the UA's attributes, and in this case should involve the ServA. If it is related to the GIdP internals, they should try to solve the problem or involve the GIdP SysA (L2support) or problem Management (L3 support), as needed.

5.8 ServA signalling a GIdP WI problem to Incident Management

Roles involved: GIdP ServA, Incident Management, <GIdP SysA>, <Problem Management>.

Description: A ServA contacts the Incident Management (L1 support) in the GN2 service desk for a problem with his usage of the GIdP WI. The L1 support should try to solve the problem, or involve the GIdP SysA (L2support) or problem Management (L3 support), as needed

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

6 Conclusions

The GIdP roles and services described here provide a comprehensive support coverage for all users of GIdP in the period it is expected to be active (that is, until eduGAIN is fully rolled out).

The overall resource estimates for the provision of this service are:

- 0.25 Person Months (PM) per User Administrator.
- 0.1 Full-Time Equivalent (FTE) for the GIdP Service Administrator.
- 0.1FTE for the GIdP System Administrator (plus approximately one week to install each GIdP instance).
- 0.2 FTE (plus 2 PM initial document writing) for the Incident Management support.
- 0.3 FTE for Problem Management (L3 support).

7 References

- [1] GEANT2 deliverable DS3.14.1 - GÉANT2 Identity Provider (GIdP) Design
- [2] http://wiki.geant2.net/pub/SA3/Sa3GidpMain/GIdP_WI_User_Admin_Guide1.2-MMrev.doc
- [3] <http://cbt.geant2.net/repository/gidp/gidp-useradmin/player.html>
- [4] <http://wiki.geant2.net/bin/view/SA3/GidpInstallationNotes2>
- [5] GEANT2 deliverable DJ5.2.2,2: GÉANT2 Authorisation and Authentication Infrastructure (AAI) Architecture
- [6] <http://www.perfsoanr.net>
- [7] <http://www.geant2.net/server/show/ConWebDoc.2544>

Project:	GN2
Deliverable Number:	DS3.14.6DS3.14.6
Date of Issue:	20/03/08
EC Contract No.:	511082
Document Code:	GN2-08-052v2

8 Acronyms

AuthN	Authentication
AuthZ	Authorization
GIdP	GEANT Identity Provider
GIdP-WI	GEANT Identity Provider Web Interface
ServA	(GIdP) Service Administrator
SysA	(GIdP) System Administrator
UA	(GIdP) User Administrator