



20-05-2010

Deliverable DS3.3.1: eduGAIN service definition and policy Initial Draft



Deliverable DS3.3.1

Contractual Date:	31-03-2010
Actual Date:	20-05-2010
Grant Agreement No.:	238875
Activity:	SA3
Task Item:	T3
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	NORDUNET/UOGOTH
Document Code:	GN3-10-081
Authors:	J. Howlett (JANET); V. Nordh (University of Gothenburg) W, Singer (Dante)

Abstract

This Deliverable describes the goals of SA3 Task3 eduGAIN. It defines the services eduGAIN provides to the GÉANT community, the models it uses to provide those services, and the policy members agree to when using the eduGAIN services.

Table of Contents

Executive Summary	1
1 Introduction	2
2 eduGAIN Service Overview	3
2.1 Service scope	3
3 The eduGAIN Model	4
4 eduGAIN Stakeholders	5
4.1 The GÉANT Project	5
4.2 Partners	6
4.3 Federation Member Organisations	6
4.4 International Partners	7
4.5 End-users	7
5 eduGAIN Governance	8
5.1 NREN PC	8
5.2 Technical Steering Group	8
5.3 Operations Team	9
6 eduGAIN Components	10
6.1 The Participating Federations	10
6.1.1 The eduGAIN/Federation Relationship	10
6.1.2 The Federation/Member Relationship	11
6.1.3 The Member / Member Relationship	11
6.2 The Metadata Distribution Service	12
6.2.1 eduGAIN / Federation Interactions	12
6.2.2 Federation / Member Interactions	12
6.2.3 Member / Member Interactions	12
6.3 The Service Desk	13
6.3.1 Support for eduGAIN members	13

6.3.2	Federation / Member Interactions	13
6.3.3	Member / Member Interactions	13
6.4	The Operations Team	13
6.4.1	eduGAIN / Federation Interactions	14
6.4.2	Federation / Member Interactions	14
6.4.3	Member / Member Interactions	14
7	eduGAIN Policy (initial draft)	15
7.1	Membership Agreement	15
7.2	Draft and Outline of eduGAIN Policy	15
7.3	Technical specifications and recommendations	16
8	References	17
9	Glossary	18

Table of Figures

Figure 1: eduGAIN Model	4
-------------------------	---

Executive Summary

The purpose of this document is to inform the service managers of GÉANT partner federations about the GÉANT eduGAIN service. This document provides a high-level description of the eduGAIN service's technical, policy and operational model. It is not intended as a final policy, but represents an initial draft and outline of the policy.

This document also describes the value of the eduGAIN service to stakeholders, including the GÉANT project, the participating partner federations and their users.

Federation service managers will obtain sufficient information and knowledge to understand the implications and benefits of participating in the eduGAIN service, and where more information may be sought if necessary.

1 Introduction

The eduGAIN service is part of the GÉANT Service Area, supporting the needs of GÉANT's own services and those of its partners. Its aim is to enable users to easily access resources and content on a pan-European scale, by connecting the Research & Education federations in a secure manner by providing a common and actively supported platform supporting the predominant industry standards for federated authentication and authorisation.

The purpose of this document is to provide Federation Service Managers with:

- A high-level understanding of eduGAIN.
- A brief description of the value of eduGAIN.
- A brief description of the eduGAIN model.
- Sufficient information to understand what is necessary to participate in eduGAIN (e.g. resources, policy, stakeholders).
- Where to go to find more information.

Section 2 provides an overview of the eduGAIN service. Section 3 provides a description of the eduGAIN model. Sections 4 and 5 describe the stakeholders and parties involved in the service. Section 6 provides a brief description of the eduGAIN policy.

Please note that this document is not intended as a final policy, but represents an initial draft and outline of the eduGAIN policy. More information about the service is available in the eduGAIN Policy and eduGAIN Business Case documents, which will be made available on the eduGAIN website [[eduGAIN](#)].

2 eduGAIN Service Overview

The eduGAIN service aims to establish a confederation of identity providers, enabling member organisations associated with different federations to securely exchange information.

There are many different federated systems in use across Europe, all of which are designed to control access to networks and applications, and ensure the secure movement of information within that network. It is currently necessary for organisations to join one another's federation in order to establish the relationship necessary to exchange information across these systems.

The existence of multiple federations makes it technically and administratively difficult for a user to access services offered by different institutions (e.g. outside of their own federation) and log on securely. When a user attempts to gain access to protected resources and services from other federations, they must first be successfully authenticated by their home AAI and then authorised by the visited Service Provider.

The aim of eduGAIN) is to enable different federations to interact.

The information needed for locating entities in the different federations is centralised at a "Metadata Service", where it can be dynamically queried and updated.

By removing the logistical burden of connecting to foreign networks and dealing with unfamiliar systems, eduGAIN allows users to focus on their work, providing access to the resources they need.

2.1 Service scope

Initially the eduGAIN Service will support Web Single Sign-on (SSO). Single Sign-on enables users to log in to multiple services, provided by different federations, using a single, one-step log-on process.

Once Web SSO is in place, the eduGAIN service will work on use-case that requires non-web SSO and other services, such as non Web-based sign-on.

3 The eduGAIN Model

Figure 1 below provides a high-level overview of the eduGAIN model, illustrating the basic eduGAIN components and their relationship.

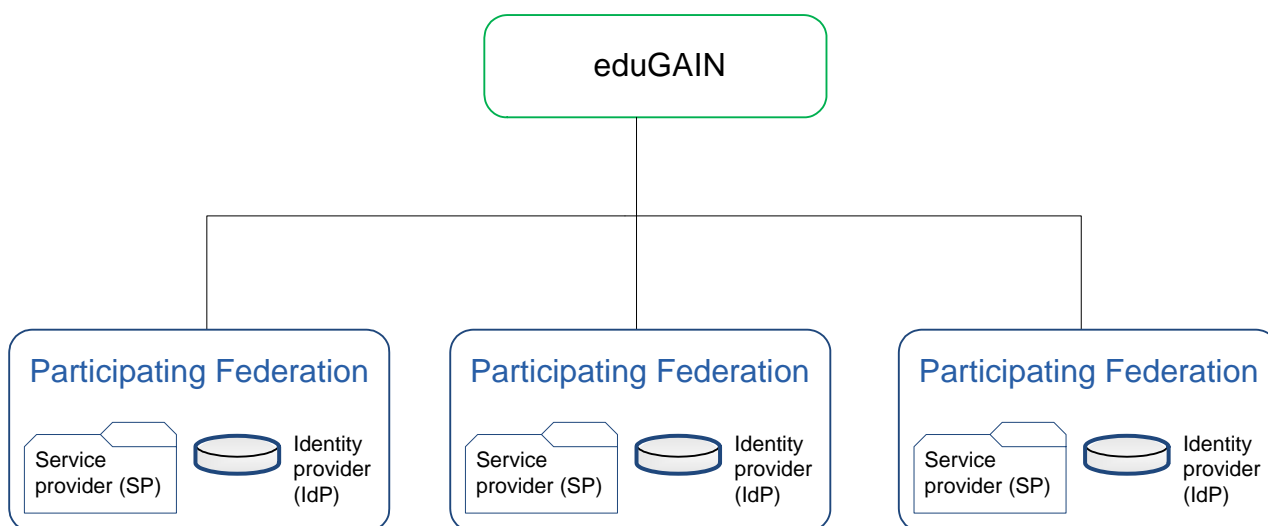


Figure 1: eduGAIN Model

Members of participating federations are able to communicate with each other and share metadata via a secure and trusted interaction. The sharing of metadata between federations enables end-users to benefit from a single sign on approach, which provides one-step login to all services provided by the federations.

The recommended technology for use between federations participating in the eduGAIN service is the OASIS Security Assertion Mark-up Language (SAML). The eduGAIN service does not attempt to regulate the use of this or other protocols within the federations.

4 eduGAIN Stakeholders

eduGAIN is being developed in conjunction with the following stakeholders:

- GÉANT Project.
- Project's Partners.
- Partners' federations.
- Member organisations associated with these federations.
- Project's international partners.
- End-users.

These stakeholders are described in the eduGAIN Business Case, which will be made available on the eduGAIN website [\[eduGAIN\]](#).

This section briefly summarises the value that the eduGAIN service delivers to these stakeholders and how this is provided.

4.1 The GÉANT Project

GÉANT is a pan-European data network dedicated to the research and education community. Together with Europe's national research networks, GÉANT connects 40 million users in over 8,000 institutions across 40 countries. The project develops and operates services of common interest to its partner NRENs. These services often have requirements for a Pan-European federated identity, principally for the purposes of authentication and authorisation.

eduGAIN provides the following benefits to GÉANT:

- Satisfies GÉANT's requirements for Web Single Sign-On (SSO). This addresses the current requirements of some of the GÉANT services.
- Provides an extensible federation platform for GÉANT to address other existing and future service requirements, such as non-Web SSO.

These benefits are provided through:

- A common technical framework for interconnecting federations.
- A common policy framework for controlling the use of this technical framework.
- A governance structure allocating responsibilities for day-to-day operations and strategic development.

4.2 Partners

At the present time, there are eighteen partners in Europe who operate federations that are eligible for participating in the eduGAIN service. There are currently two test beds, with a small number of federations performing interoperability testing. These federations facilitate access to Web-based content and resources provided by, and to, their member organisations.

eduGAIN provides the following benefits to its partners:

- Enables interconnectivity between the GÉANT partner federations, enabling federations to address the requirements of concrete use-cases at a very modest expenditure of resources.

These benefits are provided through:

- A common technical framework that closely matches the federation's technical environment.
- A common policy framework that is closely aligned with the federation's existing policy regimes.
- A service desk and operations team providing technical support and maintenance of the service.
- Technical infrastructure to enable the exchange of federation metadata between participating federations.
- Support and marketing material related to the use of the eduGAIN service.

4.3 Federation Member Organisations

It is estimated that there are approximately 1500 organisations connected through the project partners' eighteen federations. The majority of these are Research and Education institutions, but also include many commercial and non-commercial organisations providing services to these institutions.

eduGAIN provides the following benefits to member organisations from partners' federations:

- Enables interconnectivity between member organisations associated with different partners' federations. This expands the potential users of the service and allows identity providers to offer access to a greater number of service providers, subject to authorisation.

These benefits are provided through:

- A common technical framework that closely matches the member organisations technical environment.
- A trust that the participants in the eduGAIN service is related to.
- Support and marketing material for the NREN from eduGAIN.

4.4 International Partners

A number of the project's international partners have established federations; notable examples include InCommon, operated by Internet2, and the Australian Access Federation. Some of the partners are known to have established dialogues with these international partners to discuss the possibility of inter-federation.

eduGAIN provides the following benefits to its international partners:

- Provides a common vehicle for establishing interconnectivity with international partners, subject to further business and technical developments.

These benefits are provided by joining the project's partner federations in a common interfederation, which will simplify future interconnectivity.

4.5 End-users

The end-users, in this context, are the end-users of the partners' and international partners' federations. The end-users are highly representative of their constituencies, and include students, teachers, researchers, administrators and support staff.

eduGAIN provides the following benefits to its end-users:

- Enables end-users to access resources provided by members of federations participating in eduGAIN.

These benefits are provided by offering a platform on top of Service Provider (SP) and Identity Provider (IdP) interconnect.

5 eduGAIN Governance

The eduGAIN service and policy will be governed by the NREN Policy Committee (PC), with support from the Technical Steering Group (TSG) and Operations Team (OT). The eduGAIN task proposes the following governance model, which is subject to approval by the NREN PC.

5.1 NREN PC

The NREN PC is responsible for:

- Approving changes to the eduGAIN constitution,
- Decisions on peering with other confederations,
- Approving technical and other Policy documents, if they are required for Participant Federations (i.e. can force a Participant Federation out of eduGAIN),
- Approving joining of new Federations, if they are not operated by a GÉANT network and project partner,
- Other tasks defined in the Policy.

Any issue with material, legal or policy implications will be a matter for the NREN PC. Data protection and eligibility are the responsibility of the NREN PC, as are mandatory technical requirements that might preclude participation by partners.

The NREN PC delegates technical issues to the Technical Steering Group, but retains immediate responsibility for the eduGAIN service's legal and policy framework.

5.2 Technical Steering Group

Each federation nominates a delegate to the TSG. The TSG is responsible for:

- Preparing issues for approval by NREN PC.
- Approval of documents which do not need approval by NREN PC (such as, recommended and optional profiles).

5.3 Operations Team

The Operations Team (OT) is responsible for:

- Daily technical issues in eduGAIN.
- Receiving enquiries about eduGAIN and forwarding them to the appropriate body.
- Receiving and processing applications to join eduGAIN.

6 eduGAIN Components

The components in the delivery of the eduGAIN service include: the participating federations, the metadata distribution service, the Service Desk and the Operations team.

6.1 The Participating Federations

The eduGAIN service is made up of federations that have agreed to interconnect with each other. This interconnection is regulated by the eduGAIN policy (see *Section 6*), and enabled by a centrally-managed technical infrastructure.

The federations are initially expected to be GÉANT3 partners, but it is recognised that it may also be desirable for other education and/or research focussed federations, subject to approval from the NREN Policy Committee, from within Europe and elsewhere, to participate. For example, it is possible that a partner's constituency may have two or more federations related to education. It is also anticipated that the eduGAIN service may, at some future stage, inter-federate with other International partners' federations. The eligibility rules of the eduGAIN service will be described in the eduGAIN policy.

The recommended technology for use between federations participating in the eduGAIN service is the OASIS Security Assertion Mark-up Language (SAML). The eduGAIN service does not attempt to regulate the use of this or other protocols within the participating federations.

The expected uses of the eduGAIN service are federated management of access to, and the personalisation of, Web-based services. The scope of the eduGAIN service will be extended in the future to accommodate more advanced use-cases, such as non Web-based services.

6.1.1 The eduGAIN/Federation Relationship

Federations must agree to the eduGAIN policy in order to participate. The eduGAIN Technical Steering Group (TSG) approves the applications of applicant federations.

The available metadata of participating federations will be published through the eduGAIN Metadata Service. Participating federations publish metadata from their own federations to the eduGAIN Metadata Service and make the eduGAIN metadata available to its own member organisations. Participating federations can choose the entities that are published to, and obtained from, eduGAIN. This is mediated through the metadata service described in Section 5.2. It is expected that participating federation's practices will vary in this respect, but that this is a purely local policy matter. The metadata distribution processes within a federation is out of the scope of the eduGAIN service.

Participating federations are required to provide the contact information as defined in the eduGAIN policy (see *Section 6*).

Participating federations are required to co-operate on resolving technical issues associated with, for example, the eduGAIN Metadata Service.

eduGAIN provides a Service Desk, as described in Section 5.3. The Service Desk can be used by participating federations to report issues concerning the operation of the centrally-managed components of the eduGAIN service.

6.1.2 The Federation/Member Relationship

Participating federations must only publish metadata to eduGAIN for entities that are members of that federation. These members must be bound by that federation's rules.

6.1.3 The Member / Member Relationship

Member organisations of participating federations should consider carefully the assumptions they make about member organisations in other federations, who will be bound by different rules when interacting with other member organisations. This is likely to differ from the assumptions they might make about member organisations in their own federation, because other organisations are not bound by the same federation rules. There may also be variations in practice owing to the diversity of the GÉANT Service Area. For example, different federations often proscribe different semantics for attributes, therefore member organisations should not assume that an attribute obtained from a member organisation of another federation has the same meaning as the attribute obtained from a member organisation of the same federation.

Despite these variations, member organisations can make certain assumptions about members of other participating organisations; details can be derived from the eduGAIN Policy. These assumptions include:

- All entities will be accurately registered.
- Identity Providers will be associated with the Research and Education sectors.
- There will be contact information for participating entities.
- There will be efficient and fast response to abuse and technical issues.

In many circumstances it will be necessary for members to have an agreement controlling their relationship. In general, this practice should not differ from those agreements that member organisations within the same federation would typically have with each other. For matters relating to data protection, the eduGAIN policy will contain an optional data protection profile intended to address some of these issues.

6.2 The Metadata Distribution Service

The Metadata Distribution Service (MDS) is responsible for the periodic collection of member federation metadata and the subsequent aggregation and re-publishing of this metadata. The audience for this service are the entities within member federations.

The metadata is used to describe the communication endpoints that entities within member federations can use to communicate with each other as well as carry other information associated with these endpoints.

6.2.1 eduGAIN / Federation Interactions

The metadata documents from each member federation are periodically fetched from the participating federations and processed into a combined confederation document containing all of those entities published by each federation that are valid and that wish to participate in eduGAIN.

The central metadata aggregator will provide a well-known URL with all entities of all the configured federations in a single metadata document that can be obtained by participating federations.

6.2.2 Federation / Member Interactions

Federations provide metadata, which incorporates eduGAIN entities, for consumption by their members. The federation collects entity metadata from members, following locally established practices.

Members provide their entity metadata to their participating federations, following the local federation registration practice. Members consume metadata provided by their federation and can validate this metadata in accordance with the guidelines of their participating federation.

6.2.3 Member / Member Interactions

Federation entities use the metadata provided by their own federation, negating the need for any member interaction directly with the MDS. Service providers within member federations may use eduGAIN metadata to provide a local discovery service instead of utilising the discovery service provided by their federation.

6.3 The Service Desk

The primary goal of the eduGAIN service desk is to support the participating federations and act as a single point of contact for eduGAIN-related questions. Most questions are expected to be resolved at once by the service desk, with a smaller number of questions being forwarded to the eduGAIN Operations team or the eduGAIN developers for further investigation. The service desk also maintains and updates the documentation on the eduGAIN service and makes this available to the federation's operators.

6.3.1 Support for eduGAIN members

The service desk accepts, verifies that the applicant federation has their policy aligned with the eduGAIN policy and forwards applications for eduGAIN membership to the eduGAIN Technical Steering Group, with a recommendation as to acceptance.

The service desk provides support to the participating federation's operators. However, if there are issues that need to be resolved between members in different federations, these members will normally escalate their questions to the participating federation's operators.

6.3.2 Federation / Member Interactions

Issues between a member and its federation would normally be resolved by the member and its federation, although the service desk will provide assistance in exceptional cases.

6.3.3 Member / Member Interactions

Normally there are no direct interactions between a member and the eduGAIN Service desk.

6.4 The Operations Team

The primary goal of the eduGAIN operations team is to maintain and support the necessary infrastructure needed for operating and running the eduGAIN service. This includes monitoring the central components of the eduGAIN service and acting on security incidents, as described in the eduGAIN policy.

The operations team is also responsible for the maintenance and operation of the GÉANT IdP.

6.4.1 eduGAIN / Federation Interactions

The eduGAIN operations team set up and operate the MDS software, which collects the participating federations metadata. Upon request, the eduGAIN operations team provides technical assistance to enable participating federations to join eduGAIN.

6.4.2 Federation / Member Interactions

Issues between a member and its federation are normally resolved directly between the parties, without requiring the support of the eduGAIN operations team, although the operations team will provide assistance in exceptional circumstances.

6.4.3 Member / Member Interactions

There are normally no direct interactions between a member and the eduGAIN operations team.

7 eduGAIN Policy (initial draft)

The purpose of this section is to provide an overview of the initial draft of the eduGAIN Policy. For detailed information on this policy, refer to the eduGAIN policy, which will be made available on the eduGAIN website [[eduGAIN](#)].

The eduGAIN policy is the framework for provision of the eduGAIN service, including the objectives of eduGAIN, who is eligible to join, and the responsibilities and rights of the participating federations. The policy is currently being drafted and is subject to approval by the NREN PC.

The policy has the following components:

- Membership agreement or declaration, signed by joining federations.
- eduGAIN policy, approved by the NREN PC.
- Technical specifications and recommendations, which are approved by eduGAIN Technical Steering Group.

7.1 Membership Agreement

The membership agreement is a short document (1-2 pages), which is signed by a federation wanting to join eduGAIN. The agreement sets out the essential terms of the eduGAIN service, such as liability and jurisdiction. For other policy-related issues, the agreement refers to the eduGAIN policy approved by the NREN PC.

It is still to be decided if the membership agreement is a bilateral agreement, signed by the joining federation and Dante (GN3 coordinator), or a unilateral declaration signed and published by the joining federation.

7.2 Draft and Outline of eduGAIN Policy

The eduGAIN policy will contain the essential terms of the eduGAIN service. It will cover the fundamentals of eduGAIN, such as who can join it and what is the joining process, how policy violations are handled and how disputes are resolved.

The eduGAIN policy will also introduce attribute related guidelines, such as which attributes are recommended to be made available for eduGAIN-enabled end users. Because releasing attributes is often considered as processing personal data in the directive 95/46/EC on data protection, an optional profile will be introduced to help identity providers and service providers to be conformant with the directive and its local implementations.

The quality of identity and authentication in eduGAIN relies on the quality of identity management processes in the identity providers. Where the identity providers are connected to eduGAIN only via participating federations, the policy provides some recommendations on how identities are managed and end users authenticated in their home organisations.

7.3 Technical specifications and recommendations

The Technical Steering Group (TSG) will address issues of a highly technical and specific nature. These will be issues, essentially, of technical interoperability, requiring attention by subject matter experts. For example, SAML 2.0 protocol profiles, metadata profiles and other documents and recommendations of a technical nature.

8 References

[eduGAIN] www.edugain.org/

9 Glossary

AAI	Authentication and Authorisation Infrastructure
IdP	Identity Provider
MDS	Metadata Distribution Service
NREN	National Research and Education Network
NREN PC	National Research and Education Networks Policy Committee
Participant Federations	Federation participating in the eduGAIN service.
SAML	Security Assertion Mark-up Language
SP	Service Provider