



eduGAIN Policy Framework Constitution



Last updated: 29-04-2011
Activity: SA3 Task 3
Document Code: GN3-10-326
Authors: Mikael Linden, Brook Schofield, Shannon Milsom

Document Revision History

Version	Date	Description of change	Person
1.0	29-04-2011	Approved by NREN PC 21-03-2011	M Linden

Table of Contents

1	Introduction	4
1.1	Overview	4
1.2	Terms	5
1.3	Goal	6
2	Governance and Governing Bodies	7
2.1	NREN PC	7
2.2	GEANT executive	7
2.3	Technical Steering Group	8
2.4	Operational Team	8
3	eduGAIN Membership	9
3.1	Requirements for Participant Federations	9
3.2	Joining Process	9
3.3	No Express Right of Communication	10
3.4	Leaving eduGAIN	10
3.5	Policy Framework Violation	10
4	Attributes and Data Protection	11
4.1	Attribute Profile	11
4.2	Data Protection	11
5	User Experience, Branding and Intellectual Property	12
5.1	Branding eduGAIN for the End Users	12
5.2	Trademarks	12
6	Quality of Identities and Authentication	13
7	Audits 14	
7.1	eduGAIN Operations	14
7.2	Operations of Participant Federations	14
7.3	Members	14
8	Documents Supplementing the Constitution	15

9	Other Issues	16
9.1	Dispute Resolution	16
9.2	Updating this Constitution	16

1 Introduction

1.1 Overview

This document is the constitution of the eduGAIN service, defining how the service is governed and what procedural and technical requirements are mandatory for Participant Federations. This document, the profiles supplementing it and the eduGAIN Policy Declaration, which must be signed by Participant Federations, form the Policy Framework of the eduGAIN service. The Participant Federations commit to the Policy Framework when they sign the Policy Declaration to join eduGAIN.

eduGAIN is an authentication and authorisation infrastructure for cross-national access to network services, focusing initially on European level. The eduGAIN service enables Participant Federations to inter-federate. Participant Federations primarily serve the interests of research and education sectors.

eduGAIN provides an infrastructure for establishing trusted communications between Entities, such as Identity and Service Providers, in different Participant Federations. End users authenticate at Identity Providers and get access to Service Providers. Technically, eduGAIN is managed by aggregating and distributing signed SAML 2.0 metadata files.

An Entity is always registered by a Participant Federation which will use an appropriate mechanism to ensure that an Entity is only exposed to eduGAIN provided it is willing to interfederate.

1.2 Terms

AAI	Authentication and authorisation infrastructure.
Attribute Provider	An organisation which is responsible for managing additional identity data (attributes) for end users authenticated by a Home Organisation. Also a server that is acting in an Attribute Provider role as defined in SAML 2.0. In this document, an Attribute Provider refers to an attribute provider who is a Member of a Participant Federation and whom the Participant Federation has exposed to eduGAIN.
DANTE	Delivery of Advanced Network Technology to Europe. The GÉANT network is managed by DANTE.
Entity	Entity means an AAI endpoint described with a SAML 2 Entity Description. For example, an Entity can be an Identity Provider, a Service Provider or an Attribute Provider. In this document, an Entity refers to an entity that a Participant Federation has exposed to eduGAIN.
Federation	Identity federation. An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
GÉANT	The pan-European data network dedicated to the research and education community. The GÉANT network is managed by DANTE.
GÉANT Exec	Authority for supervision of the GN3 Project is delegated by the NREN PC to the Executive Committee (Exec) which runs the project at an executive level.
GN3 Project	The next phase of the GÉANT Project following on from the GN2 Project set out in the proposal submitted by the coordinator (DANTE) on behalf of the European consortium of NRENs for a grant agreement under the Seventh Framework Programme (Research Infrastructures: INFRA-2008-1.2.1-GEANT) submitted to the Commission in April 2009.
Home Organisation	The organisation with which the end users are affiliated. It is responsible for managing end users' identity data (attributes) and authenticating them. The Home Organisation is responsible for setting up and operating one or more Identity Providers, either by itself or via an outsourced service. In this document, a Home Organisation refers to a home organisation who is a Member of a Participant Federation and whose Identity Provider the Participant Federation has exposed to eduGAIN.
Identity Provider	A server acting in an Identity Provider role as defined in SAML 2.0 specifications. In this document, an Identity Provider refers to the Identity Provider that a Participant

	Federation has exposed to eduGAIN.
Member	Any organisation that has signed an agreement with a federation operator to cover the verification and publication of metadata. In this document, Member refers to a member whose Entity is exposed to eduGAIN.
NREN PC	The governing body of the European consortium of NRENs. It consists of appointed representatives from each consortium member.
OT	eduGAIN Operational Team, as defined in section 2.4.
Participant Federation	A Federation which has passed the joining process defined in section 3.2.
Policy Framework	eduGAIN Policy Framework. This document, the profiles supplementing it and the eduGAIN Policy Declarations signed by Participant Federations.
SAML	Security Assertions Markup Language (Organisation for the Advancement of Structured Information Standards).
Service Provider	An organisation that is responsible for offering the end user the service s/he is going to log in to. Also a server that is acting in a Service Provider role as defined in SAML 2.0. In this document, a Service Provider refers to a service provider who is a Member of a Participant Federation and whom the Participant Federation has exposed to eduGAIN.
TSG	eduGAIN Technical Steering Group, as defined in section 2.3.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.3 Goal

The goal of eduGAIN is to support the constituency of National Research and Education Networks by providing a service which enables Federations to inter-federate.

2 Governance and Governing Bodies

In the current form the governance is not fully representative of the situation in the service area. The intention of the current governance structure is to get the service operationally up and running in the short to medium term and to find a long term solution to its governance.

2.1 NREN PC

The NREN PC is responsible for:

1. Approving changes to this constitution.
2. Approving new technical profiles and other documents in the Policy Framework if they are REQUIRED for Participant Federations (in other words, they can exclude a Participant Federation from the eduGAIN service).
3. Approving major updates to the profiles and documents described in item 2 (in other words, if the updates are likely to affect any Participant Federation's membership in the eduGAIN service).
4. Other tasks delegated to the NREN PC in supplementing profiles.

2.2 GÉANT Exec

The GÉANT Exec is responsible for:

1. Preparing issues for approval by the NREN PC.
2. Approving minor updates to the profiles and documents the NREN PC has approved (in other words, the updates that are not likely to affect any Participant Federation's membership in the eduGAIN service).
3. Decisions on peering relationships.
4. Approving the membership of new Federations.
5. Approving Participant Federation's disqualification or temporary suspension of eduGAIN membership in case of Policy Framework violation, as defined in section 3.5.

6. Processing appeals by Participant Federations whose Policy Framework violation the OT has reacted to, as defined in section 3.5.
7. Other tasks delegated to the GÉANT Exec in supplementing profiles.

2.3 Technical Steering Group

Each Participant Federation SHOULD appoint a delegate and deputy to the TSG. The TSG's term is two calendar years. It is responsible for:

- Preparing issues for approval by the GÉANT Exec.
- Approving branding instructions, if any, for the Members, as defined in section 5.1.
- Approving documents that do not need approval by the NREN PC (such as RECOMMENDED and OPTIONAL profiles).
- Accept or amend the plan for audits of eduGAIN operations, as defined in section 7.1.
- Other tasks delegated to the TSG in supplementing profiles.

2.4 Operational Team

The Operational 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.
- Preparing an audit plan on the request of the TSG or the GÉANT Exec.

The eduGAIN task of the GN3 Project appoints the OT.

3 eduGAIN Membership

3.1 Requirements for Participant Federations

Participant Federations MUST:

- Primarily serve the interests of the education and research sector.
- Provide a point of contact for their Members for dealing with technical issues.
- Provide processes for handling complaints and incidents involving their Members.
- Have a published Metadata registration practice statement.
- Add a reference to the eduGAIN Policy Framework Metadata Terms of Access and Use document to any eduGAIN metadata file it publishes.
- Have an appropriate mechanism to ensure that only Entities which have been opted in by a Member and which are in conformance with the Policy Framework are exposed to eduGAIN.

3.2 Joining Process

The process to join eduGAIN is as follows:

1. To apply for membership, the applicant Federation signs the eduGAIN Policy Declaration and presents it to the OT.
2. The OT confirms that the applicant Federation fulfils the requirements in section 3.1.
3. Unless the GÉANT Exec has decided that the applicant Federation does not need further approvals, the OT prepares and presents a proposal to the TSG which, in turn, presents a proposal to the GÉANT Exec to approve or reject the application.
4. When an applicant is approved, the OT takes the necessary technical steps to register the Federation to eduGAIN.

3.3 No Express Right of Communication

For an Entity registered in an eduGAIN Participant Federation it does not imply any right of communication with any other Entity exposed to eduGAIN.

An individual Participant Federation or Home Organisation MAY decide not to communicate with a Service Provider exposed to eduGAIN. An individual Participant Federation or Service Provider MAY decide not to communicate with an Identity Provider exposed to eduGAIN.

3.4 Leaving eduGAIN

When a Participant Federation leaves eduGAIN:

- It MUST notify its own Members with sufficient notice to allow them to make alternative arrangements with Entities which other Participant Federations expose to eduGAIN.
- It MUST give one month's written notice to the OT, which forwards the notice to the other Participant Federations.

3.5 Policy Framework Violation

In the event of:

- A Participant Federation's severe Policy Framework violation
- A Participant Federation's Policy Framework violation which is continuous and not fixed despite several requests sent by the OT

the OT will react in one of the following ways, depending on the level and duration of violation:

- Issue a notice to the TSG.
- Issue a notice to the TSG and propose to the GÉANT Exec a temporary period of suspension.
- Issue a notice to the TSG and propose to the GÉANT Exec a disqualification of the participant federation from eduGAIN.

The Participant Federation may appeal this decision to the GÉANT Exec.

Following a decision by the GÉANT Exec to suspend or disqualify, the OT will:

- Announce suspension or disqualification of eduGAIN membership to all Participant Federations and
- Make technical changes necessary to implement the decision.

4 Attributes and Data Protection

4.1 Attribute Profile

To promote interoperability, it is important that Members have a common definition of the basic attributes exchanged in eduGAIN. This covers both the syntax and semantics, including the vocabularies. A listing of these attributes and a common definition for them will be covered in a supplementary profile.

4.2 Data Protection

Releasing end users' attributes may be considered as processing personal data. Therefore, the requirements imposed by the directive 95/46/EC on data protection and its eventual successors and national laws need to be covered. Participant Federations should ensure that Members take this into account and take necessary steps. Guidelines assisting Members will be provided in a supplementary profile.

5 **User Experience, Branding and Intellectual Property**

5.1 **Branding eduGAIN for the End Users**

The TSG MAY provide branding instructions covering end user interfaces that Members in Participant Federations SHOULD follow.

5.2 **Trademarks**

eduGAIN is a trademark of DANTE (Delivery of Advanced Network Technology to Europe) and is used under license by the Participant Federations in conjunction with the eduGAIN service. DANTE is responsible for managing and protecting the trademark.

6 Quality of Identities and Authentication

Home Organisations **MUST** have the technical and organisational means to resolve disputes relating to users that they authenticated. Participant Federations **MUST** ensure that Members (such as Home Organisations) provide only user information that is up-to-date (for example, Affiliation values) to other Members (such as Service Providers) in eduGAIN. Further guidelines on authentication and user information quality will be covered in a supplementary profile.

7 Audits

7.1 eduGAIN Operations

The OT proposes a plan for audits of eduGAIN operations, such as the centrally provided services and related processes which are accepted or amended by the TSG.

7.2 Operations of Participant Federations

In eduGAIN's basic level of trust, there are no audit requirements for Participant Federations. The Policy Framework may be amended to support enhanced levels of trust.

7.3 Members

In eduGAIN's basic level of trust, there are no audit requirements for Members. The Policy Framework may be amended to support enhanced levels of trust.

8 Documents Supplementing the Constitution

The NREN PC approves and the OT publishes technical profiles and other documents which are **REQUIRED** for participant federations.

The TSG approves and the OT publishes technical profiles and other documents which are **RECOMMENDED** or **OPTIONAL** for participant federations.

9 Other Issues

9.1 Dispute Resolution

For dispute resolution between the Participant Federations or a Participant Federation and the eduGAIN service, the OT is the first point of contact.

If the Participant Federation is not satisfied with the OT and its resolution, a Participant Federation should bring the issue to the attention of the body that nominates the OT, as defined in section 2.4.

9.2 Updating this Constitution

When the NREN PC approves a change to this Constitution, a written notice must be sent to all Participant Federations. The change becomes effective three months after sending the notice.

The OT ensures that up-to-date Policy Framework documents are published and available to the Participant Federations.