eduGAIN Policy Framework Constitution

Version date	Editor	Change
20.9.2010	ML	Changes based on the Call for Comments

1. Introduction

1.1. Overview

This document is the constitution of the eduGAIN service, defining how the ~~eduGAIN confederation~~ service is governed and what procedural and technical requirements are mandatory for ~~the~~ Participant Federations. This document, the profiles supplementing it and the eduGAIN Policy D~~d~~eclaration which has to be~~s~~ signed by Participant Federations form the Policy Framework of the eduGAIN service. The Participant Federations have committed to the Policy Framework when they have signed the Policy Declaration to join ~~joined~~ eduGAIN.

eduGAIN is an authentication and authorisation infrastructure for cross-national access to network services, focusing initially on European level. The eduGAIN service enables ~~is a confederation that interconnects~~ Participant Federations to inter-federate.~~,~~ Participant Federations primarily ~~represent~~ serve ~~ing primarily~~the interests of ~~national~~ research and education ~~and research~~sectors.~~ in a certain country.~~

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.

~~Identity and Service Providers~~Entities are always registered to the Participant Federations, which may make them visible via eduGAIN. Participant Federations are expected to apply an opt-in principle, in other words, ~~Providers~~ Members are expected to take an active step to ~~get~~ have their Entities~~be~~ exposed ~~to~~via eduGAIN.

1.2. Terms

AAI	Authentication and authorisation infrastructure.
Attribute Provider~~s~~	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. ~~Entity responsible for supplying a subject's identity attributes to other providers and relying parties.~~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 ~~service~~ described with a SAML 2 EntityDescription ~~and registered in a Participant Federation~~. An Entity can be, for instance, 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 in order to enable collaborations and transactions.
GÉANT	Gigabit European Academic Network project, the pan-European data network dedicated to the research and education community. The GÉANT network is managed by DANTE.

~~Participant Federation~~	~~A Federation which has been granted membership of eduGAIN as defined in this constitution~~
Home Organisation	The organisation which the end users are affiliated to and which is responsible for managing end users' identity data (attributes) and authenticating them. Home Organisation is responsible for~~of~~ setting up and operating either one or more ~~an~~ Identity Providers, either by itself or via~~as~~ an outsourced service. In this document, a Home Organisation refers to a home organisation who is a ~~member~~Member of a Participant Federation and whose Identity Provider ~~a~~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 Policy Committee of the GÉANT network and project, which consists of appointed representatives from each partner in the project. It is responsible for setting and overseeing overall policy of the GÉANT network and project.
OT	eduGAIN Operational Team, as defined in section 2.3.
Participant Federation	A Federation which has passed the joining process defined in section 3.3.
Policy Framework	(eduGAIN Policy Framework) This document, the profiles supplementing it and the eduGAIN Policy ~~declarations~~ Declarations signed by Participant Federations.
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 ~~that~~ ~~a~~ Participant Federation has exposed to eduGAIN.
~~NREN PC~~	~~The Policy Committee of the GÉANT network and project, which consists of appointed representatives from each partner in the project. It meets at least three times a year, and is responsible for setting and overseeing overall policy of the GÉANT network and project~~
TSG	eduGAIN Technical Steering Group, as defined in section 2.2.~~Technical Steering group, as introduced in this document~~
~~OT~~	~~eduGAIN Operational Team, as defined in section 2.3Operational team, as introduced in this document.~~

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 ~~operating~~ providing a service ~~confederation~~ which enables federations to ~~interconnecting~~ inter-federate~~Participant Federations~~.

2. ~~Confederation G~~G~~g~~overnance and governing bodies

Unless otherwise stated, governing bodies make decisions with a simple majority.

2.1. NREN PC

NREN PC is responsible for:

- approving changes to this constitution,
- decisions on peering with other confederations,
- approving technical profiles and other~~ Policy~~ documents in the Policy Framework, if they are REQUIRED for Participant Federations (i.e. can ~~force ~~exclude a Participant Federation ~~out of~~from the eduGAIN service),
- approving ~~joining ~~the membership of new Federations, if they are not operated by a GÉANT network and project partner,
- approving Participant Federation’s disqualification or temporary suspension of eduGAIN membership in case of Policy Framework violation, as defined in section 3.6,
- processing appeals by Participant Federations whose Policy Framework violation OT has reacted to, as defined in section 3.6,
- processing Participant Federation’s dissatisfaction to OT, as defined in section 9.1, and
- other tasks ~~defined in the Policy~~delegated to the NREN PC in supplementing profiles.

2.2. Technical Steering Group

Each Participant Federation SHOULD nominate a delegate and deputy to the TSG. TSG's term is two calendar years, and it is responsible for:

- preparing issues for approval by NREN PC,
- approval of branding instructions, if any, for the Members, as defined in section 5.1,
- approval of documents which do not need approval by NREN PC (such as, RECOMMENDED and OPTIONAL profiles), and~~.~~
- other tasks delegated to the TSG in supplementing profiles.

2.3. Operational Team

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.
- prepare an audit plan on the request of the TSG or NREN PC

The ~~GN3~~ eduGAIN Task Leader or his successor nominates OT.

3. ~~Confederation~~ eduGAIN membership

3.1. Eligibility to join

Following Federations are able to join eduGAIN and become a Participant Federation:

- Federations operated by GÉANT network and project partners,
- other Federations approved by NREN PC.

3.2. Requirements for Participant Federations

Participant Federations MUST:~~ at least~~

- primarily ~~represent primarily~~ serve the interests of the education and research sector~~in a certain country~~,
- provide a point of contact for their Members~~Home Organisations and Service Providers~~ for ~~sorting out~~dealing with technical issues,
- provide processes for handling complaints and incidents involving their ~~Home Organisations and Service Providers~~Members,
- have an appropriate mechanism to ensure that only ~~Identity and Service Providers~~Entities which have been opted in by a Member ~~opted-in~~ and which are in conformance~~ing~~ ~~to~~ with the Policy Framework are exposed to eduGAIN~~. As a clarification, Participant Federations do not have to expose all their Providers to eduGAIN~~.

3.3. Joining process

Joining eduGAIN has the following process:

1. To apply for membership, the applicant Federation signs the eduGAIN Policy Declaration~~inter-federation declaration~~ and presents it to the OT.
2. OT confirms that the applicant Federation fulfils the requirements ~~above~~in section 3.2.
3. For the applicant Federations not operated by a GÉANT network and project partner, OT prepares and presents a proposal to TSG which, in turn, presents a proposal to NREN PC to approve or reject the application.

4. If an applicant is approved the OT takes the necessary technical steps to register the Federation to eduGAIN.

3.4. Right to opt out

~~Membership ~~For an Entity registered in an eduGAIN ~~Federation that is a ~~Participant Federation ~~in eduGAIN confederation~~it does not imply any right of communication ~~between ~~with any other Entity exposed to eduGAIN~~particular Identity Provider and Service Provider~~.

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

3.5. Leaving eduGAIN

When a Participant Federation leaves eduGAIN,

- it MUST notify its own M~~m~~embers with sufficient notice to allow them to make alternative arrangements with ~~any Identity and Service Providers in~~Entities which other Participant Federations expose to eduGAIN,
- it MUST give a one months written ~~-~~notice to OT, which forwards the notice to the other Participant Federations.

3.6. Policy Framework violation

In case of

- a Participant Federation's severe Policy Framework violation, or
- 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 the following way, depending on the level and duration of violation

- issue a notice to the ~~the ~~TSG, or
- issue a notice to the TSG and propose to NREN PC a temporary ~~quarantine ~~period of suspension, or
- issue a notice to the TSG and propose to NREN PC a disqualification of the participant federation from ~~the confederation~~eduGAIN~~.~~

The Participant Federation may appeal this decision to the NREN PC. Following a decision by the NREN PC to suspend or ~~terminate~~disqualify, the OT will

- announce suspension or ~~termination ~~disqualification of eduGAIN membership to all ~~Participating~~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 ~~Home Organisations and Service Providers~~Members have a common definition of the basic attributes exchanged in eduGAIN. This covers both the syntax and semantics~~ of attributes~~, including the vocabularies. A listing of these attributes and a common definition ~~of attributes~~for them will be covered in ~~the Policy~~a ~~supplementing~~supplementary profile.

4.2. Data Protection

Releasing end user's attributes may be considered as processing personal data as defined in the directive 95/46/EC on data protection and its eventual successors and the national laws. eduGAIN participants ensure that Members ~~Home Organisations and Service Providers~~ take this into account and take necessary steps. Guidelines and instructions assisting ~~Home Organisations and Service Providers~~Members ~~Entities~~ will be covered in ~~the Policy~~a ~~supplementing p~~supplementary profile.

5. User experience, branding and intellectual property

5.1. Branding eduGAIN for the end users

TSG MAY provide branding instructions ~~for eduGAIN, for example,~~ covering end user interfaces, that ~~Identity and Service Providers~~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, as the organisation co–ordinating of the GN3 project, is responsible for managing and protecting the trademark.

6. Quality of identities and authentication

Home Organisations that expose Identity Providers to eduGAIN~~Participant Federations~~ MUST have the technical and organisational means to match exposed ~~ensure that~~ identities ~~in the Identity Providers are tied~~ to ~~an~~ individual end users.

Participant Federations MUST ensure that Members (e.g. Home Organisations) provide only user information that is up-to-date (for example, Affiliation values) to other Members (e.g. Service Providers) in eduGAIN. Further guidelines on authentication and user information quality will be covered in a ~~supplementing~~supplementary profile~~the Policy~~.

7. Audits

7.1. eduGAIN operations

~~DANTE agrees with~~The OT ~~on~~ proposes a plan for audits of ~~the~~ eduGAIN operations like the centrally provided services and related processes, which is 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. ~~Home Organisations and Identity and Service Providers~~ Members

In eduGAIN's basic level of trust, there are no audit requirements for ~~Home Organisations, Identity and Service Providers~~Members. The Policy Framework may be amended to support enhanced levels of trust.

8. Documents supplementing the constitution

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

TSG approves and 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 ~~the~~ eduGAIN serivce ~~confederation~~, OT is the first point of contact.

If the Participant Federation is not satisfied with OT and its resolution, a Participant Federation ~~may~~ should bring the issue to the attention of the eduGAIN Task Leader or successor ~~the NREN PC~~.

9.~~3~~2. Updating this C~~c~~onstitution

When NREN PC approves a ~~constitution~~ change to this C~~c~~onstitution, a written notice must be sent to all Participant Federations. The change becomes effective in 3 months of sending the notice.

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