

eduGAIN 政策框架——章程

(中文翻译稿, 2017 年 5 月 1 日)

文档修订记录

版本	修订日期	修订说明	作者
1.0	2011 年 4 月 29 日	2011 年 3 月 21 日 NREN PC 通过	M Linden
1.1	2012 年 11 月 14 日	政策审查期间收到的意见	M Linden
2.0	2013 年 4 月 19 日	eduGAIN-TSG 修订版本	B Schofield
3.0	2016 年 12 月 14 日	eduGAIN SG 修订版本	B Schofield & N Harris
3.0bis	2017 年 1 月 30 日	eduGAIN 政策复审编辑决定	B Schofield & N Harris
3.0ter	2017 年 5 月 1 日	eduGAIN Exec 通过 eduGAIN 政策	B Schofield & N Harris

eduGAIN 政策框架——章程

目录

1 引言	3
1.1 概述.....	3
1.2 目标.....	3
1.3 术语.....	3
2. 治理和管理单位.....	5
2.1 eduGAIN 执行委员会 (eEC, eduGAIN Executive Committee)	5
2.2 eduGAIN 指导小组 (eSG, eduGAIN Steering Group)	5
2.3 运行团队 (OT, Operational Team)	5
3. eduGAIN 成员资格	6
3.1 eduGAIN 成员资格要求	6
3.2 加入流程.....	6
3.3 参与流程.....	6
3.4 关于通信权利.....	6
3.5 离开 eduGAIN	6
3.6 暂停或取消资格的理由.....	7
4. 一般性说明.....	8
4.1 商标.....	8
4.2 争端解决.....	8
4.3 补充章程文件.....	8
4.4 更新章程.....	8
5. 参考文献.....	8

1 引言

1.1 概述

本文件是 eduGAIN 服务章程,明确了对成员联盟的服务管理方式和对成员联盟程序上的、技术上的强制要求。本文件、补充本文件的技术要求及 eduGAIN 政策声明,共同组成 eduGAIN 服务政策框架。其中政策声明需要成员联盟签署。成员联盟在加入 eduGAIN 时,签署政策声明意味着承诺遵守政策框架。这些文件由 eduGAIN 操作实践陈述 (Operational Practice Statement) 支持。声明描述了 eduGAIN 用以支持技术要求 (Technology Profiles) 运行的那些工具的完整性和可用性。eduGAIN 网页提供 eduGAIN 文件的完整文本【eduGAIN-DOC】。

eduGAIN 服务支持成员联盟之间的互相联合。这些成员联盟主要为研究和教育部门的认证和授权需求提供服务。

eduGAIN 为实体之间建立可信任沟通提供了基础设施。这些实体包括:来自不同成员联盟的身份提供者和服务提供者。用户在身份提供者处进行认证以获取服务提供者的访问权限。

一个实体由一个成员联盟来注册,该成员联盟采取一种合适的机制通过 eduGAIN 来交换实体元数据。该机制在技术要求中具体描述。

1.2 目标

eduGAIN 的目标提供一种服务,支持多个关注科研和教育的身份联盟之间的互相联合。

1.3 术语

AAI	认证和授权基础设施
eduGAIN	eduGAIN 在成员联盟之间,以提供政策框架、统一的元数据和 eduGAIN 服务共享治理的模式,实现身份、认证、授权相关信息的可信交换。
eduGAIN 政策声明 Policy Declaration	加入 eduGAIN 的联盟需要签署的协议。
eduGAIN 操作实践陈述 Operational Practice Statement	eduGAIN 集中运行了一组支持“技术要求”的工具。本文件涵盖了保证这组工具完整性和可用性的相关问题。
eduGAIN 执行委员会 eEC - eduGAIN Executive Committee	eduGAIN 执行委员会是由 eduGAIN 服务赞助方提名的一个机构,如 2.1 小节所述,负责批准 eSG 形成的决议。
eduGAIN 指导小组	eduGAIN 指导小组是由成员联盟代表组成的一个机构,如 2.2 小

eSG - eduGAIN Steering Group	节所述，它对 eduGAIN 服务负有监督职责。
实体 Entity	实体是一个 AAI 端点。例如，实体可以是身份提供者、服务提供者或是属性提供者。在本文件中，实体指成员联盟通过 eduGAIN 交换的实体元数据。
联盟 Federation	身份联盟。为了支持合作和某项事务，适度地交换他们的用户和资源的一种组织间联合。eduGAIN 中，联盟通常是由联盟运行者来代表。
联盟运行者 Federation Operator	为所属联盟的成员单位提供、调试认证和授权基础设施的机构。
联盟政策 Federation Policy	规范任何给定联盟的成员行为的一组规则、准则或过程。
GEANT	GEANT 是一个成员资格组织，和他的成员一起为他们提供服务以推进欧洲和全球的研究和教育连网。
身份所属机构 Home Organization	用户所隶属的那个机构。负责管理终端用户的身份数据（属性）并对他们进行认证。身份所属机构以自己运行或者服务外包的方式设置、运行一个或多个身份提供者。本文件中，一个身份所属机构同时是某个联盟成员的身份所属机构。
身份提供者 Identity Provider	以身份提供者角色在运行的一个系统。它以身份所属机构代表终端用户发布断言。用户通过这些断言获取服务提供者的服务访问权限。
跨联盟 Interfederation	以共享联盟元数据的形式，支持一个联盟的用户访问另一个联盟中注册的服务。
成员联盟 Member Federation	满足 3.2 小节定义的 eduGAIN 加入需求的某个联盟。
OT - Operational Team	eduGAIN 运行团队，如 2.3 小节所述。
参加者联盟 Participant Federation	积极参与 eduGAIN、满足 3.3 小节所述需求的成员联盟。
政策框架 Policy Framework	eduGAIN 政策框架。成员联盟需签署。本文件和“技术要求”是它的补充。
服务提供者 Service Provider	负责向终端用户提供服务的机构。用户通过联合登陆使用它。
技术要求 Technology Profile	“技术要求”描述如何在 eduGAIN 框架下实现指定的技术。每个“技术要求”由一个或多个文件组成，分别描述元数据产生、聚集、协议使用等具体信任功能的规则。每个“技术要求”和负责核心信任功能管理的运行团队相关联。

2. 治理和管理单位

2.1 eduGAIN 执行委员会（eEC, eduGAIN Executive Committee）

eduGAIN 执行委员会由为 eduGAIN 运行提供经费支持的机构代表组成。当前指定执行委员会和执行成员遵照 eduGAIN 网站【eduGAIN-GOV】执行。

eEC 负责正式批准 eduGAIN 指导小组 eSG 的如下决定：

1. 修改本章程。
2. 修改并提出新的“技术要求”、政策框架文件等建议。这些建议将强制每个成员联盟执行。

如果 eEC 决定不批准 eSG 的某项决定，提案将被返回给 eSG。

2.2 eduGAIN 指导小组（eSG, eduGAIN Steering Group）

eSG 是由成员联盟代表组成的团体，指导 eduGAIN 服务的发展方向。每个成员联盟应该指派一名代表和副手加入 eSG。每个成员联盟应该保证代表和副手可以代表联盟中用到的技术要求。eSG 也可以邀请不参与投票的观察员来参加会议或者加入邮件列表。

eSG 主席和不参与投票的受邀观察员任期为 2 年。eSG 负责：

1. 通过对 eduGAIN 政策框架中要求和文件的修改，比如修改或者删除某些要求或者文件。
2. 决定元数据对端关系，比如，决定和其他信任基础设施交换元数据。
3. 审核、批准新联盟的加入申请。
4. 批准如 3.6 小节所描述的关于成员联盟的取消资格或者临时暂停资格。
5. 向 eSG 指定主席和不参与投票观察员。
6. 委派给 eSG 的、补充技术要求的其他任务。

除章程修改外，eSG 决策取决于投票表决时活跃列表中大多数成员联盟的决定（见 4.4）。成员联盟可以对所有的章程修改、新的技术要求进行投票，但只能投票表决那些在他们的联盟中在使用的技术要求的修改。每个成员联盟的投票是平等的，每个成员联盟最初被认为是活跃的。连续两次缺席投票的成员联盟将从活跃名单中删除。参与投票之后，联盟可以返回活跃名单。

投票在两周内进行，但如果在那之前提前达到所需的多数，可以提前作出决定。

2.3 运行团队（OT, Operational Team）

运行团队负责：

- eduGAIN 运行的日常技术问题，如网站、集中管理的成员数据库。
- 和每一个技术要求运行者合作。
- 接收关于 eduGAIN 的询问并转发给相应单位。
- 根据 eduGAIN 政策声明，接收 eduGAIN 加入申请，审核是否符合基本要求。
- 为 eduGAIN 跨联盟服务准备并公布 eduGAIN 运行实践声明【eduGAIN-OP】，包括集中运行、各部分技术要求之间的关系。
- 根据 eSG 的要求，准备 eduGAIN 运行实践审计计划。

3. eduGAIN 成员资格

eduGAIN 在运行过程中涉及如下两类联盟：

- 成员联盟（Member Federations）已经符合 eduGAIN 加入要求，但还没有按照“技术要求”进行部署；
- 参与者联盟（Participant Federations）按照“技术要求”要求实际加入 eduGAIN。

3.1 eduGAIN 成员资格要求

成员联盟必须：

- 主要为教育和科研服务
- 提供一个联系人处理联盟成员的技术问题
- 提供联盟成员投诉和突发事件的处理流程
- 满足 eduGAIN 政策声明的要求
- 联盟和联盟成员之间签署过联盟成员资格协议（比如联盟政策）

3.2 加入流程

作为成员联盟加入 eduGAIN 的流程如下：

1. 申请提交联盟的代表在 eduGAIN 政策声明签字并提交给运行团队；
2. 运行团队确认申请联盟达到 3.1 小节的要求；
3. 运行团队准备并向 eSG 提交成员资格计划书以供审议；
4. eSG 通过投票同意或者拒绝申请；
5. 申请通过后，运行团队按照必要的步骤把这个联盟注册到 eduGAIN。

3.3 参与流程

按照技术要求，成为参与联盟的流程如下：

1. 新加入的联盟按照技术要求的相关内容公布某些文件；
2. eSG 审阅提交的这些文件；
3. 运行团队确认符合相关技术要求并将新申请联盟的符合情况公布在 eduGAIN 网站上。

3.4 关于通信权利

由某个 eduGAIN 参与者联盟发布的实体不意味着和通过 eduGAIN 交换的任何其他实体具有任何通信权利。

任何参与者联盟或身份所属机构可决定不与通过 eduGAIN 交换信息的某个服务提供者进行通信。某个参与者联盟或者服务提供者可以决定不与通过 eduGAIN 交换的某个身份提供者通信。

3.5 离开 eduGAIN

当一个联盟离开 eduGAIN 或者终止使用 eduGAIN 技术要求，必须提前一个月向 eduGAIN 运行团队提交书面申请。该申请将被转发给其他

3.6 暂停或取消资格的理由

参与者联盟可能因下列原因被暂停 eduGAIN:

- 违反技术要求的某一项。
- 违反它自己的联盟政策。
- 违反 eduGAIN 政策声明。
- eSG 不可信任投票。

当违反或问题发生时，根据违反的程度和持续时间，运行团队以以下方式中的一种或多种作出反应：

- 向参与者联盟发出通知。
- 向 eSG 发出通知。
- 建议 eSG 暂停资格。
- 向 eSG 建议取消参与者联盟的资格。
- 在适当的情况下自动中止参与者联盟。

在 eSG 决定暂停或取消资格之后，运行团队：

- 向所有联盟宣布暂停或取消 eduGAIN 成员资格，并且
- 作出必要的技术更改来执行决定。

对违反或发出的缺陷作出满意的纠正之后，运行团队：

- 向 eSG 发出通知。
- eduGAIN 恢复参与者联盟元数据。

4. 一般性说明

4.1 商标

eduGAIN 是 GEANT 注册的商标。参与者联盟在提供 eduGAIN 相关服务时许可使用。GEANT 负责本商标的管理和保护。

4.2 争端解决

eduGAIN 政策声明定义了参与者联盟之间的争端解决办法。

对于成员联盟和 eduGAIN 服务之间的争议解决，首先联系运行团队。如果成员联盟不满意运行团队及其决议，成员联盟可以把问题提交给 eduGAIN 执行委员会。

4.3 补充章程文件

eSG 批准、运行团队发布技术要求和其他章程文件。这些补充文件在 eduGAIN 操作实践声明中被引用。

4.4 更新章程

eSG 同意修订本章程的要求是活跃投票名单中至少有三分之二的联盟投肯定票。eduGAIN 执行委员会批准修改本章程，将向所有成员联盟发送书面通知。发送通知后三个月后，修改生效。运行团队确保了发布最新的策略框架文件以供成员联盟使用。

5. 参考文献

[eduGAIN-DOC] eduGAIN Policy and Technical Documents:

<http://edugain.org/policy>.

[eduGAIN-GOV] eduGAIN governance structure: <http://edugain.org/governance>.

[eduGAIN-OP] eduGAIN Operational Practice Statement:

<https://technical.edugain.org/documents>.