



**HAL**  
open science

# GÉANT “ Enabling Users ” : aide à l’adoption d’eduGAIN pour chercheurs internationaux

Thomas Bärecke

## ► To cite this version:

Thomas Bärecke. GÉANT “ Enabling Users ” : aide à l’adoption d’eduGAIN pour chercheurs internationaux. JRES (Journées réseaux de l’enseignement et de la recherche ) 2015, Renater, Dec 2015, Montpellier, France. <hal-04805396>

**HAL Id: hal-04805396**

**<https://hal.science/hal-04805396v1>**

Submitted on 26 Nov 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY-NC 4.0 - Attribution - Non-commercial use - International License

# GÉANT « Enabling Users » : aide à l'adoption d'eduGAIN pour chercheurs internationaux

**Thomas Bärecke**

SWITCH  
Werdstrasse 2  
P.O. Box  
8021 Zürich  
Suisse

## Résumé

*Les grandes communautés de recherche ne s'arrêtent pas aux frontières des États et pourtant l'organisation des infrastructures d'authentification et d'autorisation (AAI) par gestion fédérée d'identité a longtemps été enserrée dans ces limites. Depuis quelques années, le service eduGAIN du projet GÉANT élargit la portée des solutions AAI au niveau Européen voir mondial, mais son implémentation dans des cas d'usage spécifiques reste complexe et difficile. L'objectif principal de la tâche «Enabling Users» de GÉANT est d'assister les communautés de recherche dans cette démarche et de les aider à satisfaire au mieux leurs besoins en termes d'AAI avec les technologies disponibles. Dans cet exposé, nous détaillerons les objectifs, l'approche poursuivie et les résultats obtenus lors des collaborations avec plusieurs communautés de chercheurs. Il se conclut par les perspectives futures dans le cadre du projet en cours GÉANT4.*

## Mots-clefs

*Gestion fédérée des identités, eduGAIN, GÉANT, collaboration, communautés de recherche*

## 1 Introduction

La gestion fédérée des identités organisée par pays n'est pas suffisante pour résoudre les problèmes des communautés internationales de recherche. Par conséquent, le service interfédération eduGAIN, qui permet de franchir les frontières des pays, est en pleine croissance. Plusieurs fédérations (SWAMID en Suède, IDEM en Italie et aussi FER en France) sont récemment passées d'une approche « opt-in », où aucune organisation ne participe par défaut et les organisations intéressées doivent s'inscrire de leur propre initiative, à « opt-out », où toutes les organisations participent par défaut sauf si elles expriment leur désaccord explicitement. Ce changement de politique de participation a considérablement augmenté le nombre de fournisseurs d'identité. Cependant, l'implémentation d'eduGAIN dans un cas d'usage spécifique reste complexe et difficile, certaines communautés internationales de recherche ont des besoins particuliers qui ne sont pas encore pris en compte par le service et les communautés ont des différents degrés de maturité et d'expertise dans la gestion fédérée des identités. Il est donc souhaitable que les fournisseurs des infrastructures d'authentification et d'autorisation aient connaissance des besoins des communautés de recherche et réciproquement, il serait avantageux que les communautés de recherche aient une compréhension des possibilités et des contraintes des technologies existantes. Pour répondre à ces enjeux, la tâche « Enabling Users » du projet GÉANT a été créée et les JRES sont l'occasion de

présenter les objectifs, les résultats et les leçons tirées de la période 2013-2015 ainsi que nos plans pour les années à venir.

## 2 Tâche « Enabling Users »

Initiée en 2013, elle a pour but d'établir et de renforcer ces liens entre eduGAIN et les communautés de recherche. Elle s'organise autour d'une dizaine d'experts de plusieurs fédérations d'identité qui y participent activement. Les objectifs les plus importants de la tâche sont :

- Agir en tant que partenaire expert auprès des communautés de recherche souhaitant utiliser la gestion fédérée d'identités fournie par le service interfédération eduGAIN ;
- assister les communautés dans la mise en œuvre d'eduGAIN pour plusieurs services propres au projet GÉANT ;
- créer une base de connaissances d'eduGAIN pour le partage des documentations techniques orientées vers le support des besoins des utilisateurs ;
- promouvoir l'utilisation de la gestion fédérée d'identités et d'eduGAIN en général.

## 3 Collaboration avec des communautés de recherche

En mars 2013, la tâche « Enabling Users » a lancé un appel pour trouver 2 ou 3 communautés de recherche avec lesquelles elle pouvait travailler en profondeur sur des cas d'usage précis. Parmi 11 soumissions, 3 communautés ont été choisies sur la base de plusieurs critères. Dans la deuxième année du projet, 2 autres communautés ont été ajoutées. Les 5 communautés retenues et les résultats obtenus sont détaillés ci-après.

### 3.1 DARIAH

La communauté DARIAH regroupe des chercheurs en beaux arts et sciences humaines. Un objectif du projet ESFRI est de fournir une infrastructure virtuelle de recherche qui peut être utilisée par des projets électroniques des sciences humaines (« eHumanities »). Un défi particulier dans cet environnement consiste à faire participer des utilisateurs avec des connaissances techniques très variées. Les solutions proposées devaient avant tout être faciles à utiliser. En plus de la collaboration avec « Enabling Users », DARIAH a eu recours à une société de services ayant des connaissances profondes de la gestion fédérée des identités ce qui a largement facilité leur intégration. 8 fournisseurs de services (ressources web) et un fournisseur d'identités ont été ajoutés à eduGAIN. Tous ont adopté le *GÉANT Data Protection Code of Conduct*.

### 3.2 ELIXIR

Les participants d'ELIXIR effectuent des recherches en sciences de la vie et travaillent avec des données sensibles (« European Genome-phenome Archive – EGA »). L'accès est strictement contrôlé et pour cela les utilisateurs doivent être authentifiés avec grand soin. Un niveau de confiance (*Level of assurance, LoA*) a été défini et les fédérations existantes ont été analysées pour vérifier qu'elles remplissaient les conditions. Un fournisseur de service a ensuite été configuré pour n'accepter que les fournisseurs d'identités conformes aux exigences minimales. La plupart des fédérations d'identités Européennes sont dans ce sens acceptables, deux exceptions importantes sont cependant à noter, la fédération du Royaume Uni et la fédération des Etats-Unis qui, malheureusement, fédèrent beaucoup de chercheurs d'ELIXIR se trouvant dans ces deux pays.

### 3.3 Umbrella

Umbrella concerne des recherches avec des photons et des neutrons et environ 30.000 personnes utilisent les infrastructures proposées chaque année. Il a été beaucoup plus important d'établir l'accès aux services eduGAIN à partir des identités Umbrella que l'inverse. Tous les problèmes techniques, y compris l'intégration de *Moonshot* pour permettre les accès SSH et non-web, ont été résolus. Quelques problèmes administratifs et politiques restent à résoudre. En effet, certains utilisateurs d'Umbrella viennent aussi du monde des entreprises privées alors que la communauté eduGAIN se limite au monde de la recherche de l'éducation. Il est donc nécessaire de trouver un accord dans la communauté eduGAIN quant à l'inclusion ou non de ces utilisateurs.

### 3.4 CERN

Le CERN fournit une infrastructure pour des chercheurs en physique des hautes énergies. Traditionnellement, l'authentification se basait sur des certificats X.509 difficiles à utiliser. L'avantage principal est que le niveau de confiance est supérieur à celui obtenu par une identification par mot de passe. En revanche, le protocole SAML utilisé par eduGAIN est plus facile à utiliser et plus répandu dans la communauté universitaire. Un défi particulier consistait à intégrer un fournisseur d'identités Microsoft ADFS avec ses limitations par rapport aux solutions Shibboleth et SimpleSAMLphp. Plusieurs services du CERN peuvent maintenant être utilisés avec un compte eduGAIN dont disposent certains employés. Il y a eu des discussions très approfondies sur le traitement des incidents de sécurité. Elles ont concerné par exemple les procédures à suivre lors d'une usurpation d'identité très bien définies dans le monde X.509, mais pas encore au même niveau dans le monde SAML.

### 3.5 ESA : observation de la Terre

Le fournisseur d'identités et un fournisseur de service ont rejoint la fédération italienne de test dans le cadre d'un projet pilote. Le fonctionnement au niveau technique était satisfaisant, mais avant de mettre en production une solution, il a été décidé début 2015 de faire appel à un marché dédié et de séparer le fournisseur d'identités en deux.

## 4 Autres activités de la tâche

En plus du travail en profondeur avec ces 5 communautés, les responsabilités de la tâche incluent :

- répondre aux questions générales sur la gestion fédérée des identités et eduGAIN ;
- établir des relations avec des contacts internationaux dans les pays où les communautés de recherche sont les plus actives ;
- participer à des réunions ou des conférences dont l'agenda inclut le sujet de la gestion fédérée des identités ;
- donner un aperçu des possibilités technologiques et des choix architecturaux possibles aux communautés intéressées ;
- recommander des logiciels et des technologies répondant aux besoins spécifiques des communautés de recherche.

Bien que certains besoins des communautés de recherche semblent similaires, ils restent différents dans les détails. Les retours d'expérience du projet ont montré que le travail sur ces différences constituent souvent la plus grande valeur ajoutée pour les utilisateurs. L'implémentation d'un service couvrant tous les besoins de toutes les communautés en même temps amènerait à une complexité et un coût trop élevés. L'approche favorisée est donc de proposer des services adaptés aux besoins basés sur eduGAIN. Dans

certains cas, ces services existant déjà au niveau d'une fédération, ils ne nécessitent pas de travail supplémentaire, mais pour les autres besoins spécifiques, il est souhaitable de les implémenter au cas par cas sous le contrôle de la communauté en question.

## 5 Etat actuel et perspectives

La tâche « Enabling Users » va continuer son travail dans le nouveau projet GN4 qui débute au printemps 2015. Certaines demandes des communautés de recherche ont été complètement ou partiellement résolues, d'autres nécessitent encore des efforts. Par exemple, la ressource *GÉANT Data Protection Code of Conduct* a été mis en place et est utilisée pour résoudre les conflits entre les standards de protection des données et le besoin d'envoyer des attributs à l'international. Un champ de travail important encore ouvert est l'harmonisation des niveaux de confiance à l'échelle Européenne. De nombreuses autres réflexions sont en cours et elles traitent notamment de la question des autorisations d'accès aux données sensibles ou confidentielles, de l'harmonisation des niveaux de confiance ou de la question de l'autorisation d'accès aux ressources non-web.

## 6 Conclusions

La mise en place d'eduGAIN facilite les collaborations des chercheurs à l'international. Les chercheurs profitent d'une meilleure accessibilité des données dont ils ont besoin et ils ont plus de visibilité s'ils fournissent eux-mêmes des services web ou des données. La mise en place technique nécessite une grande expérience dont peu des communautés de recherche disposent parmi leurs membres. Les retours des communautés sur le travail de la tâche « Enabling Users » ont toujours été très positifs et nous ont encouragé à proposer nos services à encore plus de chercheurs. En même temps, nous apprenons beaucoup sur les besoins des chercheurs qui ne sont pas encore satisfaits et nous collaborons avec l'équipe opérationnelle d'eduGAIN pour améliorer le service. En continuant notre travail, nous proposons aux communautés de chercheurs, intéressées par des questions d'authentification et d'autorisation, différents services en commençant par des interventions ponctuelles sur des demandes d'information jusqu'à l'analyse et la conception des solutions pour des cas d'usage complexes. Nous sommes disponibles pour accorder vos besoins et nos possibilités.

## Annexe

Pour plus d'informations, vous pouvez consulter les pages web suivantes ou contactez-nous par courriel :

Projet GÉANT :

<http://www.geant.org/>

Tâche « Enabling Users » :

[https://wiki.edugain.org/Enabling\\_Users](https://wiki.edugain.org/Enabling_Users)

Data Protection Code of Conduct :

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/Pages/default.aspx>

Contact : [edugain-integration@geant.net](mailto:edugain-integration@geant.net)