MyAcademicID, pour une identité étudiante européenne unique pour l'enseignement supérieur

Hervé BOURGAULT
RENATER
23-25, rue Daviel
75013 Paris

Résumé

Le projet MyAcademicID vise à implémenter les briques de base pour l'adoption d'une identité étudiante européenne pour l'enseignement supérieur. L'objectif principal est de permettre aux étudiants en situation d'échange à l'étranger de s'inscrire et s'authentifier dans les établissements d'enseignement supérieurs, de gérer leur processus de mobilité Erasmus et d'accéder à différents services étudiant en Europe. L'infrastructure technique vouée à supporter cette identité étudiante européenne sera le résultat de l'intégration d'eduGAIN avec l'identifiant étudiant européen (European Student Identifier ou ESI), et de l'établissement de passerelles avec le cadre d'interopérabilité eIDAS, en cours de déploiement par les institutions européennes.
Le projet vise en outre à intégrer cette identité étudiante européenne dans quatre e-services liés à la mobilité étudiante : Online Learning Agreement, Erasmus+ Dashboard, Erasmus+ Mobile App et la plate-forme PhD Hub. En complément, l'identité étudiante nationale portugaise (Estudante ID) sera rendue interopérable avec l'identité étudiante européenne, démontrant ainsi la faisabilité pour un fournisseur d'identités de niveau national de rejoindre le modèle de solution proposé. Enfin, l'intégration future de la plate-forme Erasmus Without Paper est également prévue.
Le passage à l'échelle du projet et le potentiel d'intégration de l'identité étudiante européenne avec une myriade d'autres services (en ligne et hors ligne), non seulement ouvrent la voie à une mobilité facilitée des étudiants et à un renforcement du statut étudiant à travers l'Europe, mais font aussi de MyAcademicID un élément clé de l'initiative carte étudiante européenne (European Student Card Initiative) lancée par la Commission Européenne.

Mots-clefs

Mobilité Erasmus, European Student Card (ESC), eduGAIN, eIDAS, European Student Identifier (ESI)

1 Introduction et contexte

Bien que le programme Erasmus existe depuis près de trois décennies et qu'il ait connu une expansion phénoménale (passant de 11 pays participants et d'environ 3 000 étudiants en 1987 à 33 pays participants et plus de 9 millions de personnes ayant bénéficié de la mobilité sous Erasmus en 2017), les procédures en place sont restées majoritairement des procédures papier jusqu'à très récemment.

Face à ce constat et dans une optique de faciliter toujours plus la mobilité étudiante, la Commission européenne a lancé « l'initiative carte étudiante européenne » (European Student Card Initiative). Cette initiative, qui regroupe en particulier les projets carte étudiante européenne (European Student Card), Erasmus Without Paper et EMREX, a pour principal objectif de permettre aux étudiants en situation de mobilité de s'enregistrer et s'authentifier de manière sécurisée dans les établissements d'enseignement supérieurs au sein de l'Europe, en éliminant les procédures papier liées à l'enregistrement dans l'établissement d'accueil.
Le projet MyAcademicID est né sur ces fondations en y intégrant deux composantes supplémentaires que sont eduGAIN, l'interconnexion des fédérations nationales opérée par GÉANT, et eIDAS, le cadre

d'interopérabilité pour l'identification électronique en cours de déploiement par les institutions européennes. D'un point de vue stratégique, MyAcademicID revêt donc une place importante dans la mesure où il offre d'une part, une opportunité concrète d'étendre l'utilisation d'eduGAIN pour supporter les projets ERASMUS (i.e. les applications de mobilité étudiante du programme ERASMUS pourront ainsi profiter de l'automatisation apportée par la fédération d'identités) et il permet d'autre part de relancer les travaux portant sur l'interopérabilité entre eduGAIN et eIDAS, initiés sur des projets GÉANT [1] et CEF [2] par le passé.

Sur ce dernier point, il est intéressant de noter, qu'à ce jour, très peu d'universités en Europe supportent l'utilisation d'une identité électronique citoyenne de niveau national (par exemple pour la France, l'identité France Connect) pour authentifier leurs étudiants mais la plupart d'entre elles (plus de 2600) sont dans une fédération nationale (comme la Fédération Education-Recherche opérée par RENATER) et dans eduGAIN. Via MyAcademicID et le travail sur l'interopérabilité entre eIDAS et eduGAIN, les services des universités enregistrés dans eduGAIN seront à terme capables de consommer les identités électroniques citoyennes fournies par eiDAS lorsque celles-ci seront déployées à grande échelle.

Au regard de son positionnement et ses objectifs, le projet MyAcademicID est ainsi conforme à la vision européenne d'un espace européen de l'éducation, qui prévoit que, d'ici 2025, tous les étudiants en Europe devraient pouvoir faire reconnaître automatiquement leur statut d'étudiant dans les États membres de l'UE et les établissements d'enseignement supérieur, y compris l'accès aux services universitaires lorsqu'ils vont à l'étranger.

2 A propos du projet MyAcademicID

Le projet MyAcademicID vise à implémenter les briques de base pour l'adoption d'une identité étudiante européenne pour l'enseignement supérieur. L'objectif principal est de permettre aux étudiants en situation d'échange à l'étranger de s'inscrire et de s'authentifier dans les établissements d'enseignement supérieurs, de gérer leur processus de mobilité Erasmus et d'accéder à différents services étudiant en Europe.

MyAcademicID est un projet cofinancé par le programme Connecting Europe Facility (CEF) de la Commission européenne. La période de réalisation du projet est prévue sur 18 mois, de janvier 2019 à juin 2020. Le projet est piloté par l'EUF (European University Foundation) qui coordonne également le projet Erasmus Without Paper visant à numériser les principaux processus et procédures Erasmus.

Les partenaires du projet sont : European University Foundation (EUF), GÉANT, RENATER, Centre national des œuvres universitaires et scolaires (Cnous), SUNET, Direction Interministérielle du Numérique et des Systèmes d'Information et de Communication de l'état (DINSIC), Humboldt-Universität zu Berlin (UBER), University of Malaga (UMA), Direção-Geral do Ensino Superior (DGES), Fondazione ENDISU, Aristotle University of Thessaloniki (AUTH), Deutsches Studentenwerk (DSW), Ente per il Diritto allo studio Universitario dell'Università Cattolica (EDUCatt).

3 Avancée des travaux

Les premiers mois du projet ont été consacrés à l'identification/recueil des exigences et la conception d'une architecture globale pour une identité étudiante européenne pour l'enseignement supérieur.

Cette activité pilotée par GÉANT a été effectuée sous forme de plusieurs ateliers de travail qui furent utiles à toutes les parties en présence pour comprendre l'ensemble de l'écosystème (complexe) du projet, en particulier :

- comprendre le parcours (en terme d'utilisation de services) d'un étudiant en mobilité Erasmus ;
- détailler les cas d'utilisation sur les aspects authentification des différents services Erasmus inclus dans le périmètre du projet (mécanisme d'authentification existant, données étudiant utilisées, données attendues, etc.) ;
- comprendre les spécificités du service Erasmus Without Paper et son articulation avec les autres services Erasmus liés à la mobilité ;
- comprendre les différents aspects techniques du projet carte étudiante européenne ;
- détailler le fonctionnement de la fédération eduGAIN et du réseau eIDAS.

Les travaux réalisés lors de ces ateliers ont permis d'aboutir à un schéma d'architecture globale (détaillé dans la suite de ce document), qui doit permettre de fédérer les accès aux services MyAcademicID d'une

part, et d'offrir la possibilité à ces services de consommer à terme des identités citoyennes (identifiants eIDAS) d'autre part. Ce schéma d'architecture est à l'heure actuelle en cours de finalisation et servira de base pour l'implémentation et l'intégration future des différents services.

4 Architecture pour une identité étudiante européenne

4.1 De l'identification à l'authentification

Au cours des ateliers de travail, la complémentarité entre eduGAIN et la carte étudiante européenne a été mise en évidence. Alors que la carte étudiante européenne porte davantage sur l'identification de l'étudiant auprès de différents services, eduGAIN et eIDAS se concentrent quant à eux sur l'accès authentifié à des services en ligne.

En effet, il existe une multitude de services dont l'accès repose sur la capacité de l'usager à s'identifier par la présentation d'un badge reconnaissable, sous la forme d'une carte notamment. Parmi les services entrant dans cette catégorie, on peut citer l'accès aux bibliothèques ou restaurants des campus universitaires mais cela peut aussi être étendu aux transports publics, au cinéma ou au théâtre ainsi qu'à de nombreux autre services de proximité du « monde physique » qui requièrent l'identification de l'individu. Le simple fait que la personne possède la carte suffit au fournisseur de services pour lui donner accès ou lui accorder une remise. Que la personne soit celle qu'elle prétend être n'a aucune importance pour la délivrance du service.

D'un autre côté, il existe de nombreux services qui ne devraient être fournis qu'à la bonne personne. Par exemple, l'accès à mon dossier étudiant ne devrait être autorisé qu'à moi-même et éventuellement d'autres entités autorisées. Dans ce cas, l'accès authentifié au service implique la vérification de l'identité de l'utilisateur via un challenge implicite ou explicite (ex : saisie des identifiants utilisateurs) pour vérifier que la personne devant l'ordinateur est bien celle qu'elle prétend être. La force du mécanisme de vérification déterminant le niveau d'assurance (Level Of Assurance ou LOA) du processus d'authentification.

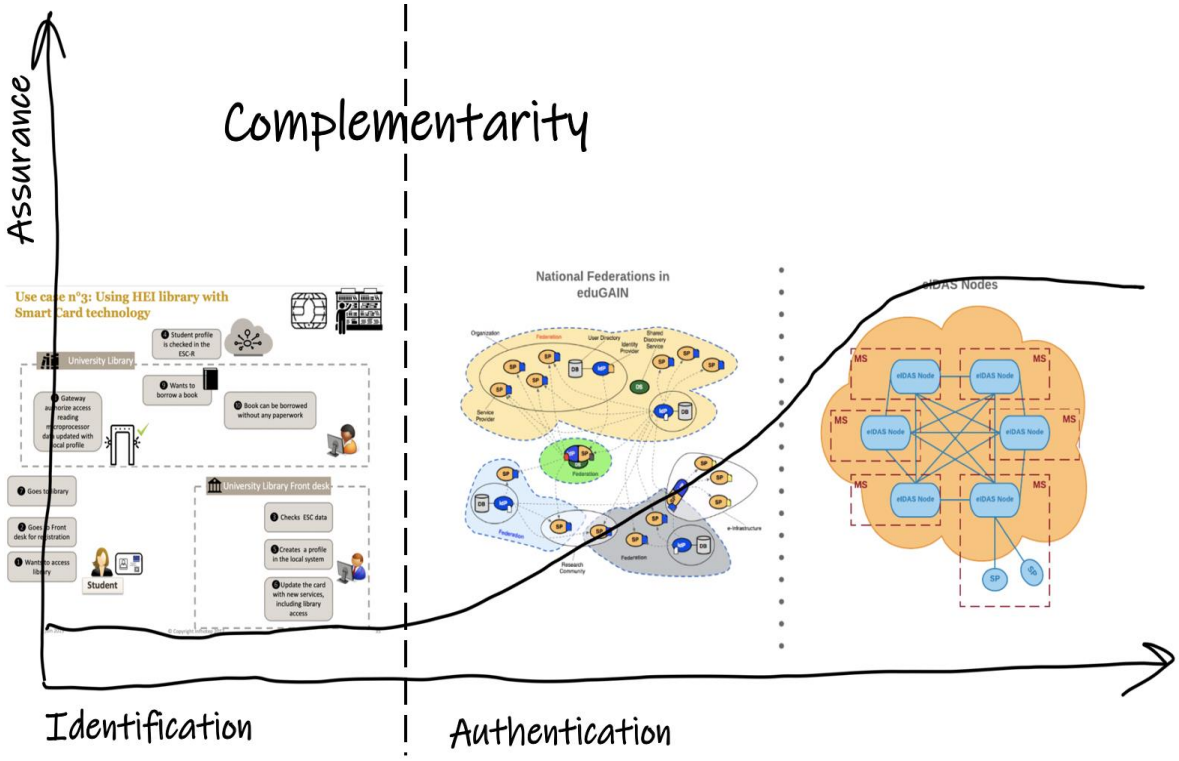

Figure 1 - Complémentarité ESC-eduGAIN- eiDAS

Dans la figure ci-dessus, sur la partie gauche, sont localisés les cas d'utilisation qui requièrent uniquement l'identification de l'étudiant mais ne nécessitent pas d'authentification. Ces cas d'utilisation sont couverts par la carte étudiante européenne qui fournit un moyen pour l'étudiant de s'identifier sur ces services.

En se déplaçant vers la droite, nous avons ensuite l'ensemble des services électroniques disponibles dans eduGAIN par l'intermédiaire des différentes fédérations nationales (par exemple la Fédération Education-Recherche). Ces services requièrent l'authentification de l'étudiant auprès de son établissement d'origine, ce qui se traduit généralement par la saisie d'un identifiant utilisateur et d'un mot de passe (fournis par l'établissement d'origine de l'étudiant). Dans le cadre du processus d'authentification, les services peuvent également demander et recevoir des informations additionnelles sur l'étudiant telles que leur nom, adresse email, affiliation, etc.

Enfin, sur la partie droite de la figure, nous trouvons les cas d'utilisation qui requièrent l'utilisation d'une identité citoyenne (ex : identité France Connect) garantissant un niveau d'assurance plus élevé pour le processus d'authentification. De plus en plus de services seront amenés à supporter ce type d'identité dans un avenir proche à mesure que leur utilisation se répandra.

4.2 Fédération des accès aux services MyAcademicID

Les services identifiés comme appartenant au périmètre du projet MyAcademicID sont :

- des services Erasmus liés à la mobilité étudiante gérés par l'EUF (European University Foundation), à savoir : Erasmus Dashboard, Erasmus Mobile App, Erasmus Without Paper, Learning Agreement Tool et PHD Hub ;
- le portail de la carte étudiante européenne (ESC Portal), géré aujourd'hui par le Cnous.

Ces services présentent certaines caractéristiques communes, mais aussi des différences importantes.
Les services Erasmus Dashboard, Online Learning Agreement, PHD Hub et le portail de la carte étudiante européenne sont toutes des applications web. Les utilisateurs doivent s'authentifier afin d'accéder à ces services et en même temps, les services doivent savoir de quelle institution provient l'utilisateur. L'application Erasmus Mobile App a des exigences très similaires à celles des services précédents, mais il s'agit d'une application mobile.

Erasmus Without Paper est autre service intervenant dans le processus de mobilité étudiante. La principale différence avec les services précédents est qu'il s'agit d'un service mettant en jeu uniquement des flux de type back-channel, sans interaction de l'utilisateur. Le service se connecte ainsi directement aux référentiels backend des établissements et peut être utilisé pour transférer les dossiers étudiants vers d'autres services Erasmus. Comme ce service n'implique aucune interaction utilisateur par nature, il ne requiert pas d'authentification de l'étudiant.

Le schéma suivant présente l'architecture globale pour fédérer l'accès à ces différents services :

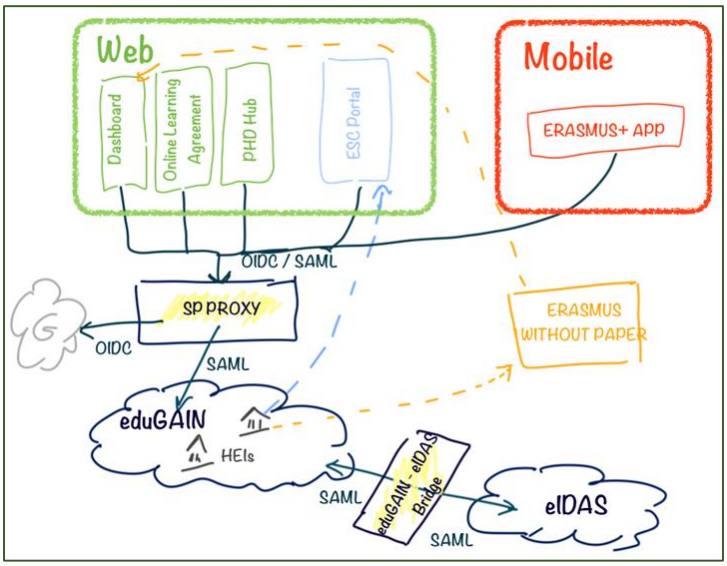

Figure 2 – Architecture globale pour la fédération des accès aux services MyAcademicID

4.2.1 Connexion des services MyAcademicID à la fédération eduGAIN

Afin de fédérer les accès aux applications web ainsi qu'à l'application mobile, nous allons les rendre disponibles dans eduGAIN au travers des fédérations nationales. Cela permettra :

1. aux étudiants : de s'authentifier auprès de leur établissement d'origine ;
2. aux services : de recevoir les informations de contact et les affiliations des étudiants fournis par leur établissement d'origine.

Les services seront connectés via un composant de type SP proxy (Service Provider proxy) multi-protocoles fourni par GÉANT, ce qui laissera la possibilité aux services d'utiliser le protocole OpenID Connect pour authentifier les étudiants via la fédération eduGAIN, qui elle est basée sur le protocole SAML.

L'utilisation du SP proxy GÉANT offre également un certain nombre d'avantages supplémentaires :

1. Il permet d'utiliser le mécanisme d'authentification existant des services Erasmus, qui est basé sur OpenID Connect.
2. Au lieu d'avoir à connecter plusieurs services dans eduGAIN, un seul service doit être connecté, le SP Proxy GÉANT.
3. La gestion de la découverte des milliers de fournisseurs d'identité actuellement enregistrés dans eduGAIN et de leurs métadonnées peut s'avérer complexe. Cette capacité sera fournie par le SP proxy, de sorte que les services n'aient pas à s'adapter à l'environnement multi-fédération et multi fournisseurs d'identité inhérent à eduGAIN.
4. Actuellement les services Erasmus utilisent l'authentification Google pour authentifier les utilisateurs. Pour gérer cet existant, le SP Proxy peut être configuré en tant que « hub d'identités » avec une capacité de liaison de comptes (account linking). Encore une fois, cette capacité est fournie par le SP Proxy pour tous les services Erasmus connectés, sans avoir à modifier quoi que ce soit côté services.

4.2.2 Connexion entre la fédération eduGAIN et le réseau eIDAS

A mesure que l'usage des identités électronique citoyennes va se généraliser, les utilisateurs devraient pouvoir s'authentifier aux services disponibles dans eduGAIN par le biais d'eIDAS, en utilisant leur identité citoyenne nationale (ex : identité France Connect).

La connexion entre la fédération eduGAIN et le réseau eIDAS sera réalisée à l'aide d'un composant de type proxy *SAML-to-SAML* (composant *eduGAIN-eIDAS bridge* sur la figure 2) qui fera office de passerelle entre ces 2 mondes. Du point de vue d'eduGAIN, le proxy apparaîtra comme un fournisseur d'identité alors que pour le réseau eIDAS, il sera vu comme un nœud de service eIDAS (eIDAS service node), comme illustré par la figure suivante :

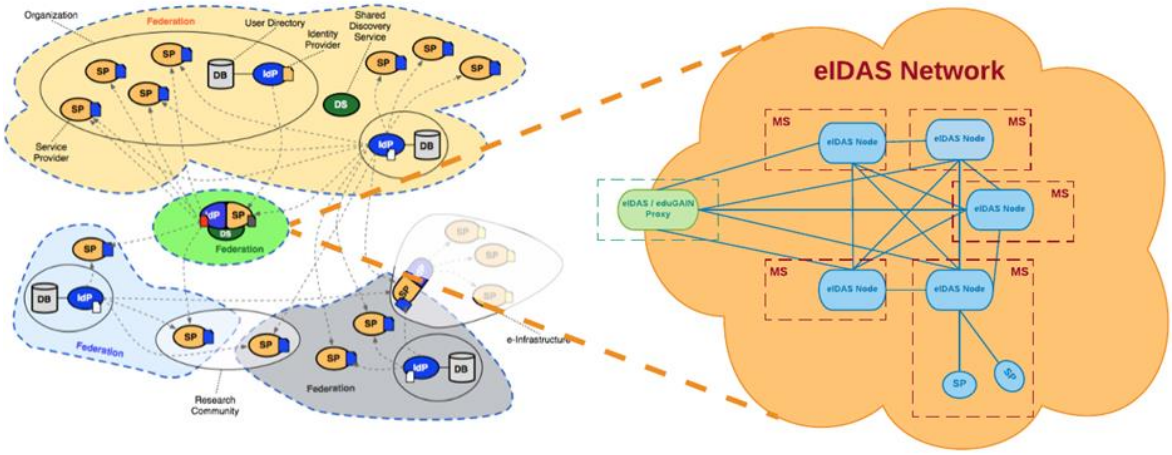

Figure 3 - Connexion entre la fédération eduGAIN et le réseau EIDAS

Dans un premier temps et afin d'avoir un prototype fonctionnel, nous implémenterons ce proxy eduGAIN-EIDAS et le connecterons au noeud eIDAS suédois (en environnement de test), géré par SUNET.
En parallèle, les discussions seront initiées avec le réseau de coopération eIDAS concernant l'intégration d'eduGAIN en tant que pays virtuel (virtual country) dans eIDAS.

4.3 L'identifiant étudiant européen

Le processus global de mobilité étudiant met en jeu plusieurs services, intervenant chacun à différents stades du processus et qui ont besoin d'échanger entre eux des données liées aux étudiants en mobilité.

Afin de pouvoir supporter un tel processus, un identifiant étudiant, pouvant être délivré par les établissements d'enseignement supérieur en Europe et partagé entre les différents services impliqués (afin d'identifier de manière unique l'étudiant) est nécessaire.

4.3.1 Exigences cibles pour l'identifiant étudiant européen

L'identifiant étudiant européen devrait être, en cible :

- **globalement unique :** chaque étudiant devrait être identifié de manière unique au-delà des frontières institutionnelles et nationales ;
- **persistant :** l'identifiant devrait suivre l'étudiant pendant la durée de ses études ;
- **non ciblé :** l'identifiant devrait être le même pour tous les services impliqués dans le processus de mobilité étudiant ;
- **indépendant du protocole :** l'identifiant ne doit pas changer de valeur en fonction du protocole utilisé. Par exemple, il devrait être le même, que SAML ou OpenID Connect soit utilisé ;
- **indépendant du transport de données :** l'identifiant ne doit pas changer de valeur en fonction du mode de transport utilisé. Par exemple, les étudiants devraient être identifiés par le même identifiant, que celui-ci soit transporté par un flux d'authentification fédéré ou par un flux back-channel entre 2 systèmes ou services.

Dans la période à venir, le projet analysera plus en détails les identifiants existants potentiellement utilisables (voir §4.3.2) et consultera les principales parties prenantes de la Commission européenne, les représentants des fédérations d'identités nationales et de l'initiative carte étudiante européenne afin de décider d'une solution pour l'identifiant étudiant européen qui respecte toutes ces exigences.

4.3.2 Identifiants existants

Identifiant issu du projet carte étudiante européenne : l'ESI

Le projet carte étudiante européenne (ESC) a déjà défini un tel identifiant, appelé European Student Identifier (ESI), qui est actuellement déployé par les universités ayant adopté la carte étudiante européenne.

Comme illustré par la figure suivante, l'ESI de la carte européenne ressemble au format bancaire IBAN, avec 4 éléments le constituant : le code pays, un code région (optionnel), un code identifiant l'établissement d'enseignement supérieur (PIC code) et l'identifiant de l'étudiant dans son établissement de rattachement (ce dernier pouvant avoir une portée locale, régionale ou nationale selon les cas) :

Figure 4 - Format de l'ESI de la carte étudiante européenne

A l'heure actuelle, l'adoption de l'ESI est limitée aux établissements pilotes du projet ESC. Une des caractéristiques intéressantes de l'ESI, tel qu'il a été défini dans le projet ESC, est qu'il permet de faire le lien directement avec l'identifiant étudiant utilisé dans les systèmes d'information des établissements (ex : l'INE pour la France). Sa limitation actuelle en revanche est liée au fait qu'il utilise un code PIC pour identifier l'établissement. La pérennité de ce dernier est en effet en question car il pourrait être remplacé par un autre identifiant établissement dans un futur proche.

Identifiants issus de la fédération d'identités et d'eduGAIN

Dans le contexte fédération/eduGAIN, un certain nombre d'identifiants utilisateur sont utilisés. Les principaux sont listés dans le tableau ci-dessous :

Identifiants	Description / Format	Exemple
eduPersonPrincipalName (ePPN)	Identifiant globalement unique pour une personne, non opaque et ré-attribuable. Composé de deux parties séparées par un « @ » : celle de gauche identifie la personne de manière unique au sein d'un établissement, et celle de droite identifie cet établissement (domaine DNS de l'établissement)	jdupont@univ-exemple.fr
eduPersonTargetedID (ePTID)	Identifiant de personne ciblé, opaque, pérenne et non-réattribuable. Constitué de 3 parties : l'entityID du fournisseur d'identité délivrant cet identifiant, l'entityID du fournisseur de service cible et un identifiant utilisateur opaque ciblé	https://idp.renater.fr/idp/shibboleth !https://evento.renater.fr !jx1SM1Be3Bn8Yg0XQ=
schacPersonalUniqueCode	Spécifie un "code unique" pour le sujet auquel il est associé. Sa valeur ne correspond pas nécessairement à un identifiant hors du champ d'application des référentiels qui utilisent ce schéma. Il peut s'agir d'un numéro d'étudiant, numéro d'employé, etc. Format de type : urn:mace:terena.org:schac:personalUniqueCode:<country-code>:<iNSS>	urn:mace:terena.org:schac:personalUniqueCode:es:uma:estudiante:a3b123c12
schacPersonalUniqueID	Spécifie un « identifiant légal » unique pour le sujet auquel il est associé. Il peut s'agir du numéro de CNI en France, DNI en Espagne, FIC en Finlande, etc. Format de type : urn:mace:terena.org:schac:personalUniqueID:<country-code>:<idType>:<idValue>	urn:mace:terena.org:schac:personalUniqueID:es:DNI:31241312L
subject-id	Nouvel identifiant omnidirectionnel à longue durée de vie, non ré-attribuable qui peut être utilisé comme clé externe globalement unique. Sa valeur pour un sujet donné est indépendante du service à qui il est transmis Format de type : <uniqueID>@<scope>	idm123456789@example.com

Figure 5 - Les identifiants disponibles dans la fédération et eduGAIN

Parmi les identifiants listés, les deux premiers (*ePTID* et *ePPN*) sont couramment utilisés dans eduGAIN mais ne répondent pas aux exigences définies pour l'identifiant étudiant européen. L'*ePTID* est un identifiant ciblé qui changera de facto d'un service à un autre alors que pour l'*ePPN* il n'y a pas de garantie qu'il ne soit pas réattribué au fil du temps. En outre, si les deux identifiants représentent l'utilisateur (étudiant) dans un contexte de fédération, c'est-à-dire tel qu'ils sont stockés dans le référentiel associé au fournisseur d'identités de l'établissement, ils ne reflètent pas forcément l'identifiant de l'étudiant qui suit celui-ci dans le système d'information de l'établissement.

Les identifiants *schacPersonalUniqueCode* et *schacPersonalUniqueID* ne sont pas couramment trouvés au niveau inter-fédération (i.e. eduGAIN) mais peuvent être plus largement répandus au sein des frontières de l'établissement ou au niveau de certaines fédérations nationales.

L'identifiant *subject-id*, comme mentionné, est un nouvel identifiant introduit récemment et son adoption est plutôt faible.

Un autre identifiant non listé ci-dessus mais qui vaut la peine d'être mentionné est l'identifiant *ORCID*. Les identifiants *ORCID* sont des identifiants persistants utilisés par la communauté des chercheurs. Leur but premier est de relier ces derniers définitivement et sans ambiguïté à leurs travaux de recherche. Les identifiants *ORCID* sont assignés, gérés et maintenus par l'organisation ORCID.

5 Perspectives

L'objectif à court terme est de finaliser l'architecture globale décrite au travers de ce document. Une première version est notamment attendue à la fin du mois de Septembre 2019.

Comme mentionné, des points restent aujourd'hui en suspens concernant le choix de l'identifiant européen ou le mode de connexion au réseau eIDAS. Afin d'avancer sur ces sujets, des discussions complémentaires seront donc menées en parallèle :

- avec l'ensemble des parties prenantes du projet (Commission européenne, représentants des fédérations nationales, Initiative carte européenne) pour choisir un identifiant répondant aux exigences identifiées ;
- avec le réseau de coopération eIDAS concernant le scénario d'intégration d'eduGAIN en tant que pays virtuel.

Sur la base du schéma d'architecture, les travaux d'intégration des services MyAcademicID vont pouvoir commencer ; les premiers résultats sont attendus fin Novembre 2019.

Enfin, afin de communiquer sur les récents développements autour de MyAcademicID auprès des futurs acteurs concernés, le projet organise une conférence qui se déroulera les 20 et 21 Novembre à Berlin. Plus d'informations sur le site web MyAcademicID.

Bibliographie

[1] C. Kanellopoulos, et coll. eduGAIN-eIDAS comparison study, Décembre 2016; https://goo.gl/tLbXE4

[2] A. Crespo, et coll. Feasibility study on cross-border use of eID and Authentication Services (eIDAS compliant) to support student mobility and access to student services in Europe, Avril 2018; https://publications.europa.eu/en/publication-detail/-/publication/b412b273-437c-11e8-a9f4-01aa75ed71a1/language-en/format-PDF/source-69424739