Gestion d'identités pour les utilisateurs en marge de la fédération du CRU : le Service d'Authentification du CRU

Mehdi Hached
Comité Réseau des Universités
CRU – Campus Centre de Ressources Informatiques
263 Avenue du General Leclerc CS 74205 Campus de Beaulieu 35042 Rennes CEDEX
mehdi.hached@cru.fr

Résumé

La fédération d'identités dans l'enseignement supérieur permet l'accès à des ressources hébergées en dehors des établissements ou partagées entre eux. Les étudiants, personnels et chercheurs des établissements inscrits en tant que fournisseur d'identités dans la fédération peuvent accéder à ces ressources de façon simple et sécurisée.

Mais quid des utilisateurs rattachés à des établissements qui ne sont pas encore fournisseurs d'identités dans la fédération ? Que faire aussi pour les utilisateurs qui n'appartiennent pas à un établissement de l'enseignement supérieur mais qui ont besoin d'accéder à des services accessibles via la fédération ?

Le CRU a développé une application, le fournisseur d'identités virtuel, qu'il opère en tant que service sous le nom de Service d'Authentification du CRU (SAC). Il permet à de tels utilisateurs d'accéder aux applications utilisant la fédération. Le SAC permet également la gestion centralisée de groupes d'utilisateurs issus d'établissements différents.

Mots clefs

Fédération d'identités, gestion d'identités, Shibboleth, SAML, authentification, autorisation, SSO, CAS.

1 Introduction

La fédération d'identités du CRU pour l'enseignement supérieur basée sur la technologie Shibboleth répond à une volonté de partage et de mutualisation des ressources dans un contexte sécurisé. Les établissements d'enseignement supérieur rejoignent progressivement la fédération en tant que fournisseur d'identités. Les utilisateurs rattachés aux établissements qui ne sont pas encore fournisseur d'identités ne peuvent pas a priori accéder aux services proposés dans la fédération. Le CRU a développé une application qu'il opère sous le nom de Service d'Authentification du CRU (SAC) afin de permettre l'accès à certaines ressources de la fédération à ces utilisateurs en marge de la fédération. Ces ressources sont par exemple des applications nationales telles que *intranet* des RSSI ou encore des services ouverts du CRU comme SourceSup. Le SAC joue donc le rôle de fournisseur d'identités temporaire pour ces utilisateurs, ainsi que pour les utilisateurs qui ne sont pas rattachés à un établissement d'enseignement supérieur. De plus, le CRU avait pour projet de développer une application de gestion centralisée de groupes. Cette fonctionnalité a donc naturellement été ajoutée au SAC ; en effet, la gestion de comptes et la gestion de groupes sont complémentaires.

2 Gestion des utilisateurs en marge de la fédération

2.1 Besoin : l'authentification

Le contexte actuel fait qu'il existe une population de personnes qui ne sont affiliées à aucun organisme fournisseur d'identités. Cette population est hétérogène mais a besoin des mêmes accès aux ressources de la fédération. On peut distinguer deux types de population.

La première population est celle des utilisateurs qui se retrouvent en marge de la fédération car ils appartiennent à des établissements qui ne sont pas encore fournisseurs d'identités au sein de celle-ci. Cette population est composée d'étudiants, de chercheurs et de personnels de ces établissements. Le SAC est pour eux un fournisseur temporaire d'identités remplaçant leur établissement d'origine dans le cadre de la fédération du CRU. Cette solution leur permet d'accéder d'ores et déjà à certaines ressources opérées par des fournisseurs de services, en attendant que leur établissement ait rejoint la fédération du CRU.

Une deuxième population est celle des utilisateurs qui ne sont rattachés à aucun établissement de l'enseignement supérieur. Par exemple, des intervenants extérieurs ou des enseignants-chercheurs étrangers. Ces utilisateurs ont besoin d'accéder à certaines ressources proposées dans la fédération et doivent donc avoir un organisme jouant le rôle de fournisseur d'identités, de façon temporaire ou définitive. Une solution serait de créer des comptes "invité" au niveau des établissements avec lesquels collaborent ces utilisateurs particuliers. La gestion des comptes "invité" est toutefois délicate, car elle peut nécessiter d'ajouter ces utilisateurs dans les annuaires des établissements et de leur créer des règles d'authentification/autorisation spécifiques, tout en gérant le cycle de vie de leurs comptes (création, mise à jour, suspension, suppression...). De plus cette solution ne fonctionnerait que pour les établissements déjà fournisseurs d'identités.

Le Service d'Authentification du CRU apporte une réponse pour ces deux populations. Ce service centralisé permet d'avoir un compte utilisateur utilisable via Shibboleth pour l'accès à certaines ressources de la fédération. Chaque fournisseur de services de la fédération gérant des ressources pourra autoriser ou non l'accès aux personnes ayant un compte CRU.

Parmi ces ressources, on trouvera les services en ligne du CRU tels que Universalistes, SourceSup ou encore des wikis. Le SAC servira aussi au remplacement du système d'authentification actuel par certificats à certaines applications nationales tels le serveur national d'anti-virus et le serveur du groupe logiciel.

2.2 Gestion de compte

Dans cette fonction le SAC joue le rôle d'organisme de rattachement (provisoire ou définitif) pour des utilisateurs n'ayant pas de fournisseur d'identités. Le SAC utilise un serveur CAS dédié pour authentifier ses utilisateurs (comme la plupart des établissements de l'enseignement supérieur français).

Un utilisateur peut se créer librement un compte CRU. C'est ce que l'on appelle le mode d'*auto-enregistrement.* Il suffit de remplir un formulaire via l'interface Web du service et après validation automatisée du compte par « email challenge », l'utilisateur est doté d'un compte. Concrètement, le service se contente de vérifier que l'utilisateur peut effectivement accéder à l'adresse email qu'il a saisi lors de la création de son compte. Ceci définit le niveau d'assurance que l'on peut attribuer à ce type de compte (cf. le chapitre 4 « Level of Assurance »). Une fois son compte activé, l'utilisateur peut s'authentifier auprès du SAC quand il a besoin d'accéder à des ressources accessibles via la fédération et qui ont accepté d'ouvrir leur accès à des utilisateurs inscrits sur le SAC.

L'identifiant d'un compte sur le service est soit un identifiant défini par l'utilisateur lui même soit son adresse email. Il aurait été toutefois préférable de forcer l'utilisation de eduPersonPrincipalName EPPN en tant qu'identifiant (EPPN est un identifiant institutionnel. En effet, celui ci est pérenne et unique au plan national. Malheureusement, la très grande majorité des utilisateurs ne connaissent pas cet identifiant et n'auraient pas été en mesure de le fournir.

3 Gestion centralisée des groupes d'utilisateurs inter-établissement

En plus de la gestion de comptes, le SAC offre une seconde fonctionnalité, distincte mais toutefois complémentaire : la gestion centralisée de groupes. L'appellation du service est volontairement axée sur l'authentification donc sur la première fonctionnalité car c'est pour elle que les besoins sont les plus pressants.

3.1 Besoin : l'autorisation

Pour contrôler l'accès à ses ressources, un fournisseur de services de la fédération s'appuie généralement sur des attributs décrivant un utilisateur. La plupart du temps la source de ces attributs est :

1. soit un référentiel d'utilisateurs local, situé au niveau du fournisseur de services ;
2. soit les attributs sont délivrés par les fournisseurs d'identités des utilisateurs via Shibboleth.

Le premier mode est celui que la fédération tend à faire disparaître afin d'éviter aux administrateurs des fournisseurs de services de gérer eux-mêmes des attributs d'utilisateurs déjà référencés dans leur établissement d'origine. Le second est quant à lui le schéma « naturel » puisqu'il s'agit du fonctionnement normal de Shibboleth : la fourniture par les fournisseurs d'identités d'attributs aux fournisseurs de services.

Certains fournisseurs de services de la fédération ont besoin d'un certain nombre d'attributs pour pouvoir filtrer les accès. Par exemple, une ressource bibliothécaire a besoin de savoir que l'utilisateur Jean Dupont de l'université X est étudiant en médecine et est bien en troisième année d'étude. Par contre, d'autres fournisseurs de services ne demandent qu'une identité S*hibbolisée.* Le SAC fournit cela. Mais ce service étant ouvert à tous, les comptes qui y sont créés n'ont aucun privilège particulier. Le SAC n'est donc pas un fournisseur d'identités comme les autres. Les attributs qu'il diffuse sont essentiellement nominatifs (nom, prénom, email) contrairement à ce que pourrait fournir une institution pour un étudiant par exemple (année d'étude, diplôme, spécialisation, etc.). Comment faire alors pour enrichir cette identité afin de faire du contrôle d'accès sur ces identités ? Cette question peut trouver une réponse dans la gestion de groupe qu'offre le SAC en tant que seconde fonctionnalité. Le SAC peut indiquer à une ressource si un utilisateur appartient à un groupe ou pas et ce sous la forme d'un attribut supplémentaire transmis via Shibboleth. Cet attribut permet à la ressource de n'autoriser l'accès qu'à un sous-ensemble d'utilisateurs ayant un compte CRU, ceux qui sont listés dans le groupe.

Cette gestion de groupe centralisée dans le SAC répond bien à la problématique suivante : l'existence dans le monde de l'enseignement supérieur et de la recherche de groupes de travail ou de collaboration constitués de membres rattachés à différents établissements. Pour illustrer, prenons des chercheurs en biologie issus de laboratoires différents qui travaillent avec des intervenants extérieurs sur un sujet bien précis. Un tel groupe collaboratif est ce que l'on appelle une organisation virtuelle (VO[1]). La gestion de ce genre de groupe ne pose pas de problème lorsque ses membres sont tous rattachés au même établissement. Ce dernier peut en effet définir ce groupe en interne avec un attribut supplémentaire dans son annuaire par exemple. Cet attribut est celui sur lequel les fournisseurs de services peuvent se baser pour contrôler l'accès à leurs ressources. Mais dans le cas où les membres sont issus de différents organismes, c'est aux administrateurs des services, auxquels ces chercheurs accèdent, de maintenir la liste des membres de ce groupe.

[1]Virtual Organization

Chaque service doit alors maintenir cette liste. On retrouve alors le problème classique de duplication et synchronisation de cette liste par chacun des services.

Le système de gestion de groupe qu'intègre le SAC répond à ce problème. Ce gestionnaire permet en effet de constituer des groupes de façon centralisée. C'est une alternative à la gestion locale des groupes au niveau de chaque fournisseur de services.

3.2 Gestionnaire de groupes

La fonctionnalité de gestion de groupe du SAC permet aux fournisseurs de services de gérer l'autorisation de façon plus fine. Elle enrichit les comptes préexistants du gestionnaire de comptes avec un attribut supplémentaire qui est l'appartenance à des groupes. Une personne peut créer un groupe d'utilisateurs via l'interface de création de groupe du service. Toute création est soumise à modération par les administrateurs du service.

Une fois le groupe validé, son gestionnaire peut ajouter des membres ou assigner d'autres gestionnaires au groupe. C'est le mode d'*enregistrement délégué* des membres. Une notification est envoyée à ces derniers pour les prévenir de leur nouvelle appartenance au groupe. Ils pourront, s'ils le souhaitent, créer leur compte CRU. Cette création est bien-sûr inutile pour les utilisateurs appartenant déjà à un établissement fournisseur d'identités.

L'appartenance au groupe apparaît dans le référentiel du SAC. Seul le gestionnaire aura besoin d'un compte CRU actif pour gérer les groupes qu'il y a créé. La référence et la gestion des groupes est donc centralisée et unique.

3.3 Gestion des attributs

La brique fournisseur de services Shibboleth a des limitations techniques concernant l'interfaçage avec les fournisseurs d'identités. Actuellement, cette brique ne peut pas recueillir des attributs concernant une même personne de deux sources à la fois. Ceci pose problème à un fournisseur de services pour l'exploitation de la gestion de groupe offerte par le SAC. Nous l'illustrons par l'exemple suivant.

Imaginons qu'un wiki ait un accès via Shibboleth réservé aux enseignants en mathématiques des universités françaises. Ce groupe d'enseignants est défini dans le SAC. Parmi les membres de ce groupe, certains utilisent leur compte CRU pour accéder au wiki. Ce dernier peut utiliser l'attribut remonté par le SAC qui spécifie leur appartenance au groupe pour contrôler l'accès. Parmi les membres du groupe, d'autres utilisent le compte de leur université pour accéder au wiki via Shibboleth. Pour eux la brique Shibboleth SP[2] n'est pas capable d'enrichir le profil utilisateur en interrogeant le SAC pour vérifier s'ils appartiennent ou non au groupe.

Pour contourner ce problème le SAC aura une interface SOAP. Elle permettra à ce wiki d'interroger le SAC sur l'appartenance d'un utilisateur à un groupe en dehors du mécanisme Shibboleth.

[2]Service Provider

À terme, on pourra se passer d'une telle interface puisque les versions futures de Shibboleth permettront aux fournisseurs de services d'enrichir un profil utilisateur en interrogeant plusieurs sources de données.

4 Level of assurance (LoA)

Le niveau d'assurance est une notion qui concerne le niveau de qualité d'enregistrement d'un profil, le niveau de l'authentification. Il est admis actuellement l'existence de quatre niveaux de LoA donc un document du NIST fait une bonne présentation [1].

Le fournisseur d'identités qu'est le SAC n'est pas inscrit dans la fédération du CRU car le niveau d'assurance de ses comptes n'est pas au niveau de ce qui est exigé par la fédération vis à vis des fournisseurs d'identités. En effet, faire partie de la fédération en tant que fournisseur d'identités oblige à certaines mesures techniques qui permettent d'obtenir un LoA plus élevé que le LoA du SAC. Ces mesures sont explicitées dans la convention d'inscription pour les IdP[3] [2]. Le SAC n'apparait donc pas dans la liste des fournisseurs d'identités proposés par le service de découverte (WAYF[4]) maintenu par chaque fournisseur de services. Dans le cas où un fournisseur de services accepte un accès via le SAC, nous recommandons de le faire apparaître dans le WAYF *auprès et non pas avec* les autres IdP. Voir sur la figure ci-dessous représentant le WAYF du CRU qui permet l'accès à certains de ses services ouverts aux comptes CRU.

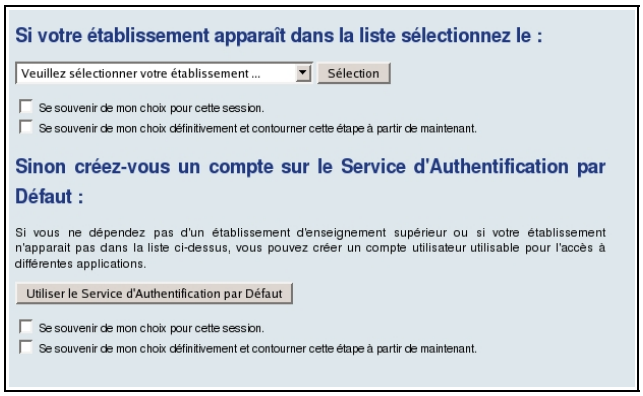

Figure 1: Service de découverte du CRU

Une université gère des annuaires type LDAP où sont répertoriés ses étudiants et son personnel avec des attributs qui leurs sont liés. Ces attributs permettent de définir un profil d'utilisateur et on peut même aller jusqu'à l'identification de ces personnes. Le SAC, lui, ne permet pas cela. Il peut juste garantir la relation entre un utilisateur donné et son adresse email. La différence entre le SAC et les fournisseurs d'identités d'établissement touche également la richesse des profils utilisateur transmis : une université peut par exemple, fournir des données nominatives, une adresse email institutionnelle (e.g. paul.dupont@etudiant.univ-francaise.fr) ou encore des

[3]Identity Provider

[4]"Where Are You From?"

données concernant les affectations pour le personnel ou les années d'études et la spécialisation pour les étudiants. Le SAC ne fournit que des données nominatives simple : nom, prénom et une adresse email (institutionnelle ou pas).

La gestion de groupe qu'offre le SAC peut remédier à cela puisque l'inscription à un groupe est modérée par le gestionnaire du groupe. Dans le SAC l'attribut d'appartenance à un groupe bénéficie donc d'un LoA plus élevé que les autres attributs décrits plus haut. Un fournisseur de services peut donc utiliser ce type d'attributs d'appartenance à un groupe pour réaliser du contrôle d'accès.

Pour résumer, même si un utilisateur possède un compte CRU, cela ne lui garantit pas l'accès à un service de la fédération. Toutefois, le LoA du SAC est suffisant pour l'accès à certaines ressources dans la fédération :

1. celles qui sont ouvertes à tout utilisateur, par exemple, certains services du CRU (Universalites ou Sourcesup) ;

2. celles dont les utilisateurs pourront s'authentifier via Shibboleth grâce au SAC, mais pour lesquelles le contrôle d'accès s'appuiera sur une autre source de données (par exemple l'interface SOAP du SAC ou une base de données centralisées).

5 Implémentation

La figure ci-dessous montre la structure du SAC.

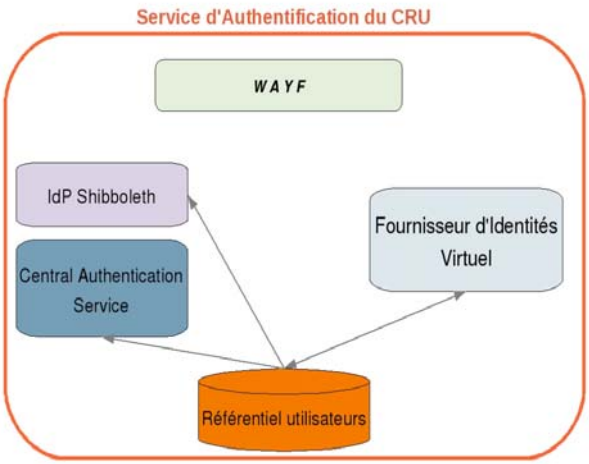

Figure 2: structure du SAC

Le SAC est un service composé de cinq briques. Il est basé sur une application appelée le fournisseur d'identités virtuel qui lui sert de cœur applicatif. C'est cette application qui alimente la base de données et gère les interactions avec l'utilisateur. Il agit en tant que fournisseur d'identités grâce à la brique IdP Shibboleth. Un serveur SSO CAS gère l'authentification. Une base de données SQL se charge de la rémanence et représente le référentiel des comptes et des groupes. Cette base est interrogée par CAS pour l'authentification des membres, par l'IdP pour en extraire les attributs et par le cœur métier pour ce qui est de la mise à jour des informations.

5.1 Le fournisseur d'identités virtuel

Le fournisseur d'identités virtuel est une application écrite en JAVA utilisant le *framework Hibernate* pour la liaison base de données/cœur applicatif et le *framework JSF* pour l'interface graphique et les interactions avec l'utilisateur. Ce produit sera distribué par le CRU. Il pourra alors être localement déployé au niveau d'un établissement ou d'une UNR[5] pour gérer des comptes invités locaux ou comme service de gestion de groupe.

5.2 Le *WAYF*

Le service de découverte est une étape essentielle qui permet à l'utilisateur de s'orienter depuis un service pour atteindre son établissement de rattachement. Chaque SP déploiera son WAYF en y faisant figurer les établissements de la fédération qu'il accepte. Si un fournisseur de services accepte un compte CRU, celui-ci pourra utiliser le WAYF du SAC en tant que service de découverte. Typiquement, le cheminement d'un utilisateur de la fédération consiste en :

1. l'accès à la ressource, clic sur le bouton «Se connecter » ;
2. choix de son établissement IdP sur la liste des fournisseurs d'identités disponibles ;
3. redirection vers le SSO CAS de l'établissement pour l'authentification ;
4. retour sur le service de façon authentifiée.

Si un utilisateur accède plusieurs fois au même service, il pourra contourner l'étape du WAYF en indiquant au WAYF quel est son établissement de rattachement. Cela sera enregistré comme préférence dans son navigateur (Cookie HTTP).

6 Conclusion

Ce nouveau service opéré par le CRU est un service d'accompagnement de la fédération. Il pourra servir de fournisseur d'identités temporaire pour les utilisateurs rattachés à des établissements qui ne sont pas encore inscrits dans la fédération, et de fournisseurs d'identités permanent pour les utilisateurs qui ne seront jamais rattachés à un établissement de la fédération.

Son rôle de fournisseur d'identités devrait prendre moins d'importance dans l'avenir par rapport à sa fonction de gestion de groupes au fur et à mesure que des fournisseurs d'identités s'intègrent à la fédération.

Le système de gestion de groupes offre quant à lui un bon moyen de gérer, toujours de façon centralisée, des groupes d'utilisateurs rattachés à des établissements différents. Des services peuvent s'appuyer dessus pour contrôler et personnaliser l'accès des utilisateurs à leurs ressources. Avec l'arrivée prochaine d'une version de Shibboleth permettant la collecte d'attributs depuis plusieurs sources

[5]Université Numérique en Région

de données, cette dernière fonctionnalité sera bien mieux intégrée dans l'architecture de la fédération.

Bibliographie

[1] National Institute of Standards and Technology, Electronic Authentication Guideline, Avril 2006. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[2] Convention d'inscription à la fédération pour les fournisseurs d'identités. http://federation.cru.fr/cru/references/convention_fournisseur_identites.pdf