

LE NOUVEAU SYSTÈME D'ACCREDITATION DES PERSONNES ET L'ACCÈS AUX APPLICATIONS SÉCURISÉES

CLAUDE.LECOMMANDEUR@EPFL.CH, SIC



Le système d'accréditation **Accred** permet aux personnes autorisées (les accréditeurs) de gérer les personnes dans les unités de l'école (facultés, instituts, laboratoires, sections) et hors EPFL (associations, PSE, ...).

Le fait pour une personne d'être accréditée dans une unité lui donne les droits d'accès aux prestations de base des services de l'EPFL, mais chaque service est le maître et décide

lui-même quelles sont les prestations qu'il donne et à qui. Le but essentiel du nouveau système d'accréditation est de permettre aux prestataires de service d'exercer un contrôle fin sur la gestion de leurs utilisateurs, sans avoir à gérer eux-mêmes ces utilisateurs.

Il faut comprendre ici les termes *services* et *prestations* au sens large, il s'agit généralement de prestations *informatiques*:

- accès à une application sécurisée;
 - accès à une simple page Web protégée;
 - accès à un login sur un ordinateur;
 - accès à un service central: adresse email, compte IMAP...
 - etc.
- mais c'est plus vaste:
- droit à une carte Camipro;
 - accès à certains locaux;
 - etc.

Pour les applications informatiques, **Accred** agit en concertation avec le serveur **Gaspar**. **Gaspar** gère l'authentification (qui est là ?) et **Accred** le contrôle d'accès (quels sont vos droits?). L'application finale (au sens utilisateur final) ne voit pas directement **Accred**, mais elle bénéficie de ses services via **Gaspar**.

Quels sont les attributs, gérés par **Accred**, pertinents pour effectuer les contrôles d'accès ?

L'UNITÉ

Une accréditation est en gros un couple (personne, unité). La personne étant connue par son numéro Sciper, et l'unité par son numéro unique d'unité. Dans une unité, peuvent être accréditées plusieurs personnes (heureusement) et une personne peut être accréditée dans plusieurs unités. Une application pourra ainsi décider de n'accepter que les utilisateurs accrédités dans une ou plusieurs unités connues d'elle.

LE STATUT

C'est le découpage le plus grossier pour différencier les personnes. Les 4 valeurs possibles sont **Personnel**, **Hôte**, **Hors EPFL** et **Étudiant externe**. Le sens de cet attribut est à peu près évident. Le statut **Étudiants** est géré directement par le Service Académique.

LA CLASSE

Ce classement est un peu plus fin, les valeurs possibles sont **Apprenti(e)**, **Stagiaire**, **Assistant(e)**, **Employé(e) technique/administratif**, **Professeur(e) / Enseignant(e)**, **Doctorant(e)**, **Secrétaire**, **Professeur(e) honoraire** et **Chargé de cours**. Je ne m'entends pas non plus là-dessus, c'est à peu près clair.

LES DROITS

Beaucoup plus intéressant. A chaque personne accréditée peut-être associée une liste de droits. En fait une liste de couples (droit, unité). On dira alors que la personne a le droit **droit** pour l'unité **unité**. Les droits sont en général des droits d'accès à des services. Par exemple:

- accéder au serveur de fichier AFS;
- faire une demande de travaux;
- ...

Les applications informatiques correspondantes peuvent demander au serveur d'authentification (**Gaspar**) de vérifier que les personnes authentifiées sont titulaires du droit correspondant lors de l'authentification.

LES RÔLES

Un peu similaires aux droits. A chaque personne accréditée peut-être associée une liste de couples (rôles, unité). Les applications peuvent aussi demander la vérification à **Gaspar**.

A chaque droit est automatiquement associé un rôle, nommé **admin-le_droit**, les personnes titulaires de ce rôle pour une unité **U**, peuvent attribuer le droit en question à toute personne, et ce, dans toutes les unités filles de **U**. On parle d'administrateur du droit.

Les rôles connus d'**Accred** sont pour l'instant peu nombreux:

- enseignant
- responsable d'unité
- responsable de centre financier
- responsable GASPARE
- accrédateur
- secrétaire
- administration du droit accès au serveur AFS
- administration du droit demande de travaux

Le rôle **Accrédateur** est utilisé par l'application **Accred** elle-même pour savoir qui est accrédateur pour quelle unité. Balaïze, non?

Donc, une application qui veut restreindre son accès, doit d'abord demander la création d'un droit associé (et donc du rôle d'administrateur correspondant), ou d'un rôle associé. A chaque connexion, elle demande à **Gaspar** d'authentifier le client, en précisant que ce client doit être titulaire du droit / rôle en question.

Si la personne n'a pas ce droit / rôle, **Gaspar** la rejette, sinon, il renvoie à l'application la liste des unités pour lesquelles, la personne a le droit / rôle, plus la liste des unités pour lesquelles la personne a le rôle d'administrateur du droit dans le cas d'un droit.

AVANTAGES DE CE SYSTÈME

L'avantage essentiel de ce système est de décentraliser la tâche et la responsabilité d'attribuer les droits d'accès, délestant ainsi les applications / services du fardeau de gérer ses utilisateurs.

Bien sûr les primitives de classement des utilisateurs offerts par **Accred** ne seront pas suffisantes pour toutes les applications, mais la palette offerte permet sans doute de répondre à beaucoup de besoins. D'autre part, l'application est vivante, toujours en développement et des extensions sont à prévoir. ■