La gestion des identités à l'Ecole Polytechnique Fédérale de Lausanne

Claude Lecommandeur

La gestion des identités à l'Ecole Polytechnique Fédérale de Lausanne

Claude Lecommandeur
Domaine IT
École polytechnique fédérale de Lausanne 1015 Lausanne
claude.lecommandeur@epfl.ch

Résumé

*Cette article a pour but de décrire les différents concepts et outils mis en place à l'EPFL ces dernières années pour la gestion des identités (Identity Management). L'accent sera mis sur le contrôle d'accès à travers les outils de gestion des droits et des rôles (**Accred**) et d'authentification Web (**Tequila**).*

La question essentielle à laquelle les applications sécurisées doivent répondre est : « Qui a droit à quoi ? ». Répondre à cette question est le plus souvent non trivial et nécessite d'accéder à des informations multiples, gérées dans des bases de données variées et parfois non disponibles de manière publique.

Il faut bien sûr pouvoir identifier et authentifier les utilisateurs, mais ce n'est en général pas suffisant, le rattachement d'une personne à une unité organisationnelle est un plus, mais souvent pas encore suffisant, il faut aussi disposer d'informations précises sur les rôles et les droits de cette personne dans son organisation.

L'EPFL compte environ 3000 employés et 7000 étudiants. Qui va pouvoir dire de manière fiable et à jour que telle personne est bien responsable informatique ou responsable communication dans telle unité ? Seules les unités elles-mêmes peuvent répondre correctement à cette question, mais il faut malgré tout disposer de cette information de manière centrale pour la redistribuer à toutes les applications autorisées qui en font la demande.

Pour répondre à toutes ces questions, nous avons mis en place une infrastructure centrale qui offre ses services à toutes les applications sécurisées, tout en prenant en charge les contraintes de sécurité et de confidentialité des données personnelles. La description de ce service central est tout le sujet de cet article.

Mots clefs

Gestion des identités, Identification, Authentification, Contrôle d'accès.

1 Introduction

1.1 Qu'entend-on par « gestion des identités »?

Toute entité (personne, ordinateur, application, etc.) qui veut accéder à des ressources à accès protégé doit :

- posséder une **identité** unique, tel un numéro de sécurité sociale ;
- s'**authentifier** en prouvant cette identité, par des données biométriques (photo, empreinte digitale), un mot de passe, un code NIP (Numéro d'Identification Personnel) associé à une carte RFID, ...
- être **autorisée** à accéder à la ressource, selon des règles établies par une autorité reconnue.

Lors d'un contrôle de police, le permis de conduire est une pièce d'identité, la photo permet d'authentifier son possesseur, et les autorisations sont délivrées par un organisme agréé.

Ces trois aspects sont regroupés en informatique sous l'appellation *gestion des identités* ou « *Identity Management* » (IdM dans la suite de cet article). Nous ne traiterons que le problème de la gestion des identités des personnes.

Créer un système informatique facilitant la vie et le travail des personnes dans un milieu devenant de plus en plus numérique est une tâche complexe et l'IdM est devenu pour l'EPFL un thème prioritaire de réflexion.

L'objet de cet article est de montrer comment nous avons abordé ce sujet ces dernières années.

1.2 Enjeu de l'IdM

Depuis quelques années, il est devenu évident que, pour toute entreprise ou institution, l'IdM est un projet qui doit être pensé **globalement**. Les **identités numériques** des personnes prennent le pas sur leur présence physique pour régler les questions de droits d'accès aux ressources, matérielles ou numériques. Les processus d'**authentification** et d'**autorisation** sont présents sur de nombreux flux d'information et voies de circulation des personnes.

L'enjeu de l'IdM est de fournir une infrastructure solide permettant aux personnes autorisées d'accéder à des services ; les spécificités d'un milieu académique comme l'EPFL rendent cette tâche plus complexe, comme explicité au point suivant.

Par ailleurs, la **sécurité informatique,** qui est une des autres préoccupations prioritaires actuelles, est très fortement liée à une bonne implémentation de l'IdM qui permet d'éviter les usurpations d'identité et délègue le contrôle au niveau des responsables des ressources.

Une personne physique est en fait représentée par un ensemble **identificateur, attributs, rôles** et **droits**. Cette modélisation est suffisante pour lui permettre d'accéder à toutes les ressources auxquelles elle a droit et seulement à celles-ci.

Exemples concrets à l'EPFL :

- Identificateur : numéro SCIPER – 6 chiffres.

- Attributs : statut (étudiant, collaborateur, invité ...), adresse-e-mail, etc.

- Rôles : responsable informatique, etc.

- Droits : réserver un billet de train, etc.

La gestion de ces données numériques est la combinaison d'un ensemble de processus (pour l'introduction et la modification des données et des règles) et d'une infrastructure technologique fiable pour la création, la maintenance et l'utilisation de ces identités.

Schématiquement, l'infrastructure IdM traite les données provenant de divers fournisseurs et les fournit aux applications consommatrices, le traitement étant régi par des règles (*Business Rules*).

1.3 Particularités d'un milieu académique

1.3.1 Structure de l'EPFL

Pour la clarté de ce qui suit, voici la structure de l'EPFL. L'école est divisée en facultés, chaque faculté est elle-même divisée en instituts, eux-même divisés en laboratoires. L'école comprend aussi des unités administratives, des associations, des entreprises externes, ainsi qu'une galaxie de structures hétéroclites. Chacune de ces entités sera référencée sous le terme d'unité.

1.3.2 Complexité et plasticité des rôles et des droits

La gestion du cycle de vie d'une personne peut s'avérer beaucoup plus **complexe** en milieu académique où la population change fréquemment de statut vis-à-vis des ressources utilisées.

Un étudiant inscrit en license est parfois un collaborateur temporaire (assistant-étudiant), ensuite il fait une année de master dans une autre université européenne, devient membre de l'association des élèves, puis il devient doctorant-assistant à l'EPFL (payé peut-être par une entreprise qui n'a rien à voir avec l'EPFL), puis travaille comme externe, mandaté par un laboratoire, puis crée son entreprise au PSE (incubateur d'entreprises), tout en donnant quelques cours en tant que chargé de cours, quitte l'EPFL, y revient... etc. Puis après une retraite bien méritée, profite encore de quelques prestations privilégiées ! À chaque période de cette vie, ses relations par rapport à l'EPFL lui donnent droit à certaines prestations, qu'il est prioritaire de ***contrôler*** *(pour éviter des abus ou des problèmes de sécurité) mais aussi qu'il faut* ***simplifier*** *au maximum pour le confort (et l'efficacité) de la personne.*

1.3.3 Délégation des responsabilités aux unités

Les tâches de recherche de l'EPFL font que l'école fonctionne du point de vue des responsabilités comme une fédération d'unités ; chaque unité a ses propres contraintes et chaque chef d'unité est responsable de son personnel, de son mode de fonctionnement, de ses finances ; les outils de gestion de l'IdM doivent donc respecter cette **autonomie** tout en garantissant la cohérence des données. Ceci ne peut se faire qu'avec des outils qui permettent une **délégation** des **responsabilités**.

D'un point de vue sécuritaire, la solution de délégation est la meilleure, elle évite les accréditations périmées, donc des droits inadéquats, et la mise en place de processus centralisés complexes, qui n'ont pas forcément les moyens de faire les vérifications nécessaires.

Des règles de fonctionnement (*policies*) sont définies de façon globale pour toute l'EPFL.

Exemples de règles définies globalement pour l'EPFL :

- les étudiants n'ont pas accès au serveur DISTRILOG (serveur de logiciels payants).

- seuls les collaborateurs de l'EPFL ont accès aux commandes en ligne de fournitures, etc.

À l'intérieur de ce cadre, les facultés sont responsables de leur politique. Les outils implémentés permettent toutes les granularités : un schéma très centralisé (seules quelques personnes sont autorisées à gérer les identités pour toute la Faculté) ou au contraire un schéma très décentralisé (dans chaque laboratoire, une (ou plusieurs) personne désignée par le responsable du laboratoire est habilitée à le faire).

C'est précisément le rôle du système d'accréditation de l'EPFL. La gestion des droits d'une personne se fait dans le contexte d'un rattachement à une unité. Ce principe est essentiel, le droit n'est actif qu'au sein de cette unité et il ne peut être donné que par une personne qui en a la responsabilité. Il n'est par ailleurs pas possible pour un responsable d'unité de donner ou enlever des accréditations pour une autre unité.

Il est très important de remarquer que le responsable qui veut donner des droits à une personne de son unité doit s'authentifier auparavant dans le système d'accréditation, et par ce biais il signera virtuellement l'accréditation qu'il va donner et en assumera la responsabilité.

De plus, comme expliqué plus loin, de nombreuses identités sont créées et détruites au niveau de l'unité qui seule est sûre des nouvelles identités et se porte garante des droits qu'elles doivent avoir. Si cette gestion des cas "particuliers", très nombreux en milieu académique, devait être centralisée, cela entraînerait des coûts et des délais importants (plusieurs échanges nécessaires avec l'unité pour s'assurer du bon droit de la demande).

1.3.4 Intégration dans un schéma suisse et international

L'EPFL n'est pas isolée du reste des milieux académiques. Les ressources de l'EPFL doivent s'ouvrir à des chercheurs et étudiants appartenant à d'autres organisations et dont l'identité numérique est gérée ailleurs ; réciproquement, nos étudiants et chercheurs ont besoin d'accéder à des ressources sur d'autres campus dont l'accès est contrôlé. Quand SWITCH [5] (réseau des universités et hautes écoles suisses) a cherché à déployer une stratégie d'AAI (*Authentication & Authorization Infrastructure*) à l'échelle de la Suisse en choisissant l'outil ***Shibboleth***, notre intégration s'est réalisée rapidement, grâce à notre infrastructure IdM déjà en place et fonctionnelle.

Au delà de la Suisse, l'EPFL devra s'**intégrer** dans d'autres fédérations où elle prévoit des échanges. Les solutions choisies par ces partenaires pourront être

hétérogènes, d'où l'importance de suivre des standards et des protocoles ouverts, pour pouvoir un jour échanger des identités avec Shangai ou Dubai !

Trois cas concrets de la réalisation de cette intégration :

*- la bibliothèque de chimie Biscom, Bibliothèque Scientifique Commune UNIL-EPFL. Les collaborateurs et étudiants de l'EPFL utilisent les outils d'authentification de l'EPFL (**Tequila**), ceux de l'UNIL (Université de Lausanne) les outils correspondants de l'UNIL.*

- OLAT, Online Learning And Training, système de gestion d'apprentissage développé par l'Université de Zurich, qui accepte les outils d'authentification de l'EPFL.

- Moodle, outil de e-learning.

1.3.5 Une population qui bouge

Tous les jours, de nouvelles personnes arrivent ou quittent le campus, parfois pour des périodes temporaires. Souvent leurs identités ne sont pas gérées par les Ressources Humaines ou le Service Académique (étudiants mobiles, chercheurs invités), mais presque toujours elles doivent pouvoir accéder à certaines ressources, donc être intégrées dans l'IdM de l'EPFL. De plus, il faut une très grande **réactivité** dans les processus car on ne peut imaginer qu'un invité attende une semaine avant de pouvoir accéder à des ressources protégées, essentielles à ses activités (locaux, documents, applications, ...), ceci tout en maintenant un niveau de sécurité optimal.

1.3.6 Multiplication et hétérogénéité des applications sources et clientes

Notre système d'information a une longue histoire et une grande hétérogénéité. Les principaux maillons ont été conçus et sont gérés par des équipes qui n'ont pas la même culture et dont les intérêts sont parfois divergents. La mise en place de notre infrastructure IdM a dû se faire dans cet environnement complexe.

D'un point de vue technique, toutes les applications du campus ne fonctionnent pas encore sur le modèle idéal où l'authentification et le contrôle d'accès sont délégués à une infrastructure centrale qui vérifie l'identité de l'utilisateur et s'il satisfait aux contraintes exigées par l'application. Certaines applications fonctionnent encore de manière totalement autonome, en dehors de toute infrastructure AAI, en gérant les autorisations en local. Ce schéma où une application gère tout elle-même est le pire du point de vue sécurité : autant de mots de passe que d'applications, une liste de personnes autorisées très vite obsolète.

1.3.7 Des contraintes qui laissent de la place à la liberté académique

Peut-on utiliser une même IdM pour sécuriser un distributeur de boisson ou accéder à une salle blanche ? Il s'agit là d'un des enjeux capital du projet : les uns souhaitent privilégier le confort d'utilisation en minimisant les contraintes imposées, les autres exigent un maximum de sécurité. L'infrastructure doit pouvoir s'adapter en permanence aux nouveaux besoins et aux nouvelles technologies en matière de sécurité.

Il est évident que toutes les contraintes de contrôle et de sécurité que l'on peut accepter dans une salle blanche ou dans une centrale nucléaire ne sont pas nécessaires au niveau des tâches quotidiennes. Il faut garder à l'esprit le principe de proportionnalité : les contraintes doivent être à la mesure des risques. Il faut donc à la fois sauvegarder le confort de l'utilisateur, lui permettre d'évoluer dans un espace de liberté, tout en garantissant la fiabilité et la sécurité.

2 Les solutions mises en place à l'EPFL

Il est important de remarquer que la démarche est, depuis le début, **modulaire, pragmatique** et **prospective** :

- modulaire : l'IdM a été conçue à l'EPFL comme un ensemble ouvert de briques interconnectées, l'accent étant mis sur les protocoles et les standards ; chaque brique pourrait d'ailleurs évoluer de façon indépendante sans nuire à la cohésion de l'ensemble ;
- pragmatique : les outils ont été développés au fur et à mesure que de nouveaux besoins sont apparus ; cette souplesse de réaction est la meilleure garantie pour l'avenir ;
- prospective : pour être prêt quand les besoins sont exprimés par la population EPFL, il fallait les anticiper et construire l'infrastructure de façon à pouvoir intégrer les nouveaux développements ;

Dans la suite, nous allons détailler les différents outils utilisés.

3 Identification

L'identification d'une personne consiste en l'attribution d'un identificateur unique à cette personne. Cet identificateur sera le plus souvent un nombre ou une courte chaîne de caractères. Cette identification est particulièrement importante quand plusieurs applications manipulent les mêmes objets : elles devront alors utiliser le même identificateur à chaque référence vers cet objet. Nous avons mis en place un système d'identification possédant toutes les qualités requise qui ne sera pas détaillé ici.

4 Authentification

L'authentification est l'action qui consiste à s'assurer de l'identité d'une personne. Pour ce faire, il faut évidemment qu'un système d'identification existe au préalable. L'authentification se fait en général au moyen d'un échange de secret, mot de passe ou certificat X.509.

Nous disposons d'un outil de gestion des mots de passe centralisé (***Gaspar*** [8]***)*** ainsi que d'une infrastructure PKI [9].

Concentrons-nous sur le problème de l'authentification Web.

Le but est de fournir aux applications Web sécurisées de l'institution un outil pour authentifier leurs utilisateurs. Elles ne doivent pas avoir à se soucier des mises à jour des

listes de personnes ou du mode d'authentification (mot de passe, certificat, etc.).

Les qualités requises pour un tel système sont :

- s'appuyer sur l'outil de gestion des mots de passe et de la PKI.
- offrir ses services à tout type d'application Web sécurisée, indépendamment de l'OS qui les supporte et du langage utilisé.
- communiquer avec d'autres infrastructures d'authentification (par exemple ***Shibboleth***).
- Support du Single Sign-On (SSO).

4.1 *Tequila*

L'outil ***Tequila*** est composé d'un serveur et de modules clients. Les applications Web sécurisées réparties dans toute l'EPFL (plusieurs centaines actuellement) utilisent les modules clients pour déléguer l'authentification de leurs utilisateurs au serveur. Seul le serveur ***Tequila*** accède aux données confidentielles des personnes. ***Tequila*** utilise les données de ***Gaspar*** pour prendre ses décisions d'authentification et supporte le single sign-on.

Le serveur ***Tequila*** accède aux données réelles des personnes via un système de '*plugins*'. Ces données réelles sont dans la pratique stockées dans un serveur LDAP et différentes bases de données MySQL et Oracle. L'authentification proprement dite s'effectue auprès d'un serveur LDAP.

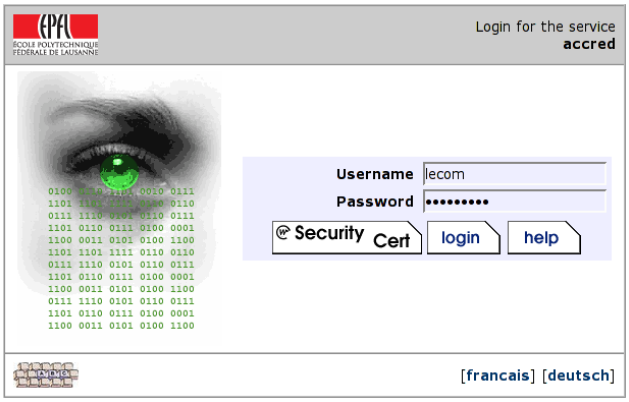

Figure 1 - *Login* ***Tequila***

Toute personne connue du système de gestion des mots de passe est reconnue par ***Tequila*** et peut accéder aux applications sécurisées si elle en a le droit.

Tequila est aussi un outil de contrôle d'accès, nous allons détailler ce point par la suite.

Plusieurs serveurs ***Tequila*** peuvent coopérer pour constituer un domaine unique ou chaque serveur pourra déléguer l'authentification effective à n'importe lequel des autres serveurs du domaine.

4.2 Intégration *Tequila - Shibboleth*

L'intégration dans une fédération ***Shibboleth*** est aussi disponible. Le serveur ***Tequila*** se comporte comme un **service provider** et un **WAYF** (Where Are You From) ***Shibboleth***. Si une application Web sécurisée veut donner des accès à des utilisateurs appartenant à une organisation membre de la fédération ***Shibboleth*** SWITCH, elle le signale au serveur ***Tequila*** et celui-ci adapte son écran de login pour permettre à l'utilisateur de choisir le serveur ***Shibboleth*** qui va l'authentifier :

TequilaAllows userClass=***Shibboleth***

L'écran de login devient :

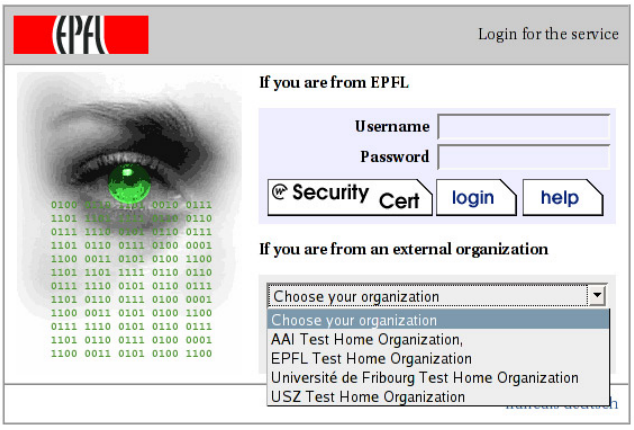

Figure 2 - *Login* ***Tequila*** *+* ***Shibboleth***

Ce système nous a beaucoup facilité la vie ; toutes les applications utilisant l'authentification ***Tequila*** bénéficient sans changer une seule virgule de l'authentification ***Shibboleth,*** et ceci sans écrire ni installer la moindre ligne de logiciel.

Dans cette architecture, le serveur ***Tequila*** est le seul serveur configuré comme Service Provider ***Shibboleth*** et tout le travail a été fait une seule fois sur cette machine. L'installation d'un client ***Tequila***, qui doit se faire sur chaque serveur supportant des applications sécurisées, est infiniment plus simple que celle d'un service provider ***Shibboleth.***

5 Contrôle d'accès

Un service doit pouvoir donner des droits différents à ses clients en fonction de différents paramètres liés à chacun d'eux. Le fameux 'Qui a droit à quoi ?'. Les personnes qui contrôlent la réponse à cette question pour chaque cas particulier sont en grand nombre et réparties dans toute l'institution. Il faut donc fournir à la personne responsable de la gestion d'un service une infrastructure lui permettant de prendre correctement ses décisions, et aux responsables des unités les moyens de gérer qui, dans son unité, peut accéder à quel service.

5.1 Gestion des rattachements, droits et rôles

Un bon modèle de gestion du contrôle est basé sur l'attribution de droits et rôles aux personnes. Un rôle donne un certain nombre de droits. Les droits peuvent aussi être

explicites, sans les rôles associés. Les rôles et droits peuvent/doivent être relatifs à des unités organisationnelles.

Le rattachement d'une personne à une unités est aussi un facteur important de décision pour le contrôle d'accès, surtout dans un contexte très diversifié comme peut l'être une institution académique ou de multiples structures cohabitent : associations, entreprises associées, etc.

5.1.1 Qualités requises :

- À chaque rôle est associé un certain nombre de droits.
- Un droit peut dépendre de zéro, un ou plusieurs rôles.
- Les droits et rôles sont attribués à des personnes **relativement** à des unités.
- Ces associations personne/droit/unité et personne/rôle/unité doivent être indépendantes des rattachements de la personne (on peut avoir des droits dans une unité où l'on a pas de rattachement).
- Gestion souple de l'attribution des droits et rôles. Il doit être possible de définir des politiques d'attribution centralisées ou décentralisées.
- Gestion souple des unités. Il existe différentes catégories d'unités (internes, externes, associations, etc.). Il doit être possible d'associer des comportements différents aux rattachements à ces différentes catégories. Par exemple, les rattachements à des associations d'étudiants ne doivent par défaut pas donner droit à des commandes de logiciels.

5.1.2 Accred

Accred est l'outil de gestion des rattachements, rôles et droits des personnes.

Chaque personne est rattachée à une ou plusieurs unités. À chaque rattachement sont associés des attributs : un statut, une classe, une fonction, etc. Ces attributs sont accessibles à ***Tequila*** et sont donc utilisables pour contrôler l'accès à des données ou des applications. Cet ensemble de rattachements, droits et rôles d'une personne constitue ce qu'on nomme une accréditation.

Figure 3 - *Un exemple de rattachement*

Les droits sont relatifs à des unités. On dit que telle personne possède tel droit pour telle unité. Les droits correspondent généralement à des applications : posséder le droit correspondant à une application permettra à la personne détentrice d'avoir accès à cette application. Par exemple, le droit « distrilog » permettra de commander des logiciels payants dans l'application éponyme.

Les rôles facilitent la gestion des droits. Détenir un rôle pour une unité, donne automatiquement tous les droits associés à ce rôle pour cette même unité, mais aussi la possibilité de déléguer ces droits à d'autres personnes.

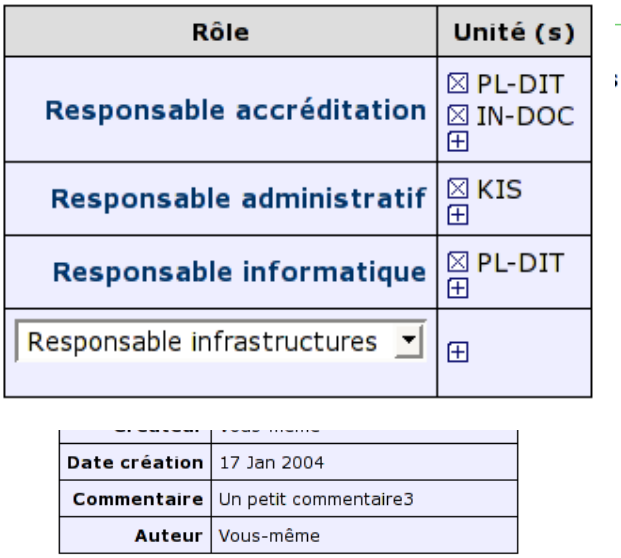

Figure 4 - Un exemple de rôles d'une personne

Accred utilise ces notions pour son usage personnel. Le rôle « Responsable accréditation » donne à son détenteur les droits « Accréditation » et « Attribution de rôles » dans les unités correspondantes. Le droit « Accréditation » permet de créer, modifier ou détruire des rattachements de personnes dans ces mêmes unités. Le droit « Attribution de rôles » permet de modifier les rôles (attribution, révocation) des personnes.

Avec ce système, le gestionnaire central d'***Accred*** ne doit in fine nommer explicitement que le responsable accréditation de l'unité EPFL, racine de l'arbre des unités et mère de toutes les unités. Cette personne (il peut y en avoir plusieurs), dispose ainsi de tous les moyens pour déléguer une partie de sa tâche au niveau des facultés, en y donnant ce même rôle pour toute la faculté. Le mécanisme se reproduit ensuite pour tous les niveaux dans la hiérarchie des unités.

De même, une personne titulaire du droit «Gestion des comptes ***Gaspar***» dans une unité pourra gérer les comptes ***Gaspar*** des personnes rattachées à cette unité ou ses descendantes dans l'arbre des unités et donc changer les mots de passe ou créer des comptes.

5.1.3 Configuration d'Accred

Dans la mesure du raisonnable, nous avons essayé de limiter le nombre des rôles, le nombre des droits étant laissé assez libre. Il n'y a que 6 rôles définis dans ***Accred***, en voici la liste avec les droits associés.

- Responsable accréditation.
  - Accréditation
  - Attribution de rôles
  - Administration des comptes ***Gaspar***
- Responsable administratif.
  - Commandes en ligne économat
  - Commandes cartes de visites
  - Commandes billets de train
  - Inventaire
  - Contrôle des services financiers
  - Gestion des instances de paiement en ligne
- Responsable communication.

  - Gestion des profils personnels
- Responsable informatique.
  - Administration des comptes ***GASPAR***
  - Accès au service DISTRILOG
  - Accès Réseau pour Hôtes
  - Services Réseau
  - Administration des accès au firewall
  - Accès au serveur AFS
  - Envoi de SMS par le Web
  - Envoi de SMS par email
  - Accès Intranet
  - Accès à l'application Inventaire
  - Administration Active Directory délégués
  - Demandes d'hébergement de machines virtuelles
  - Compte utilisateur dans l'Active Directory
- Responsable infrastructures.
  - Demande de travaux
- Responsable sécurité.
  - Aucun pour l'instant

Ces rôles sont purement administratifs et sont très stables dans le temps. Les droits évoluent très vite et de nouveaux sont créés régulièrement. De toute façon, la définition d'un nouveau droit ou d'un nouveau rôle se fait en quelques clics.

La réalisation de cette décentralisation dans ***Accred*** est très souple. Le responsable d'un institut peut ainsi décider si certains droits ou rôles seront gérés dans les laboratoires ou non, et le responsable d'une faculté pourra prendre les mêmes décisions pour ses instituts. Ce type de décentralisation pourra ainsi être adapté de manière fine pour chaque besoin de sécurité. Il faut remarquer que ce modèle de décision de proximité est un facteur de sécurité.

Accred supportant une traçabilité totale, il est toujours possible de remonter à la personne qui aurait attribué indûment un rôle ou un droit.

Accred automatise les tâches les plus fastidieuses et répétitives. Les données provenant de la gestion du personnel (SAP) et de la gestion des étudiants (IS-Academia) sont ainsi automatiquement entrées sans intervention manuelle.

5.2 Gestion des groupes et invités

Parfois, les attributs des personnes ou leurs rattachements ne sont pas suffisants pour permettre une discrimination efficace. On peut penser par exemple à des projets horizontaux, ou des groupes de travail. Il faut alors disposer d'un outil permettant de créer ex-nihilo des groupes de personnes en les énumérant explicitement. Nous avons développé une application (***Groupes***) qui effectue ce travail en collaboration avec les autres outils d'IdM.

De même, un outil spécifique a dû être développé pour la gestion des personnes externes (***Guests*** [3]).

Nous ne détaillerons pas ces 2 applications ; on pourra se référer aux sites Web en bibliographie pour plus de détails.

5.3 Contrôle d'accès Web

La majorité des applications sécurisées sont maintenant des applications Web. Il faut donc fournir à ces applications une interface commode avec l'infrastructure d'authentification et de contrôle d'accès sous-jacente.

5.3.1 Qualités requises

- Facilité d'utilisation.
- Utilisable dans tous les langages, sur tous les systèmes d'exploitation.
- Permettre la protection aussi bien des données statiques (HTML) que des scripts CGI.
- Offrir une interface complète, c'est à dire masquer totalement l'infrastructure d'authentification et de contrôle d'accès, mais en supporter tous les aspects.
- Offrir une interface avec d'autres systèmes d'authentification Web (***Shibboleth*** pour l'instant, d'autres dans le futur).

5.3.2 Tequila

Comme mentionné précédemment, ***Tequila*** est aussi une infrastructure de contrôle d'accès. Il est ainsi possible pour un client ***Tequila*** de spécifier que seuls les utilisateurs possédant tel droit, tel rôle, ou bien encore tel statut, pourront accéder à une application sécurisée. Le serveur ***Tequila*** se charge de faire les vérifications nécessaires auprès de l'application concernée (***Accred***, ***Groupes***, etc.), libérant ainsi l'application appelante de cette charge complexe qui nécessiterait de pouvoir accéder aux données de ces applications.

Tequila délivre ainsi toute la puissance du système d'information de l'EPFL à travers une interface normalisée et utilisable par tous les responsables d'applications sécurisées.

Une application qui fait appel aux ressources de ***Tequila*** peut demander au serveur de vérifier des assertions sur l'utilisateur qui s'authentifie. Dans le cas du client ***Tequila*** sous forme de module Apache, on pourra ainsi spécifier :

```
<Location/restricted/>
 TequilaAllowIf firstname=Jeanne&name=Dupont
 TequilaAllowIf group=AASL
</Location>
```

dans le fichier de configuration Apache ou dans un fichier .htaccess.

Ce qui signifie, que seule l'utilisatrice 'Jeanne Dupont' et les membres du groupe AASL pourront accéder à l'application. Le serveur ***Tequila*** se charge lui-même de cette vérification, Grâce à ceci, il est par exemple possible que le contenu du groupe ne soit pas public. On peut même aller plus loin en demandant un accès anonyme : ***Tequila*** vérifie que les assertions sont respectées, mais ne donne pas l'identité de l'utilisateur à l'application cliente.

L'interface vers ***Shibboleth*** ne détruit pas ce contrôle d'accès. Après authentification de l'utilisateur, ***Tequila*** peut effectuer des vérifications d'assertion sur les valeurs d'attributs (malheureusement peu nombreux pour l'instant dans le fédération SWITCH :)) renvoyées par ***Shibboleth***.

L'accès des clients se fait soit via un module Apache, soit au travers des modules Perl, Ruby, PHP ou Java.

6 Intégration dans le système d'information global

Beaucoup de données concernant l'IdM proviennent de bases de données périphériques : gestion du personnel, gestion des étudiants, gestion des unités, etc.

Ces données ont souvent une structure complexe très orientée métier et leur importation dans l'infrastructure IdM est un problème non trivial. Il faut se pencher en profondeur sur le sens réel de ces données pour une bonne intégration. De plus, ces systèmes périphériques changent souvent et de manière non coordonnée avec des conséquences parfois lourdes sur la fiabilité de l'IdM.

De fait, une part importante (peut-être 50%) des efforts de développement de notre infrastructure IdM est dédiée à cette tâche de communication avec le reste du système d'information.

7 Évolution de l'IdM à l'EPFL

L'évolution de l'IdM doit se faire dans la même démarche de construction modulaire, qui a démontré sa souplesse d'adaptation et sa fiabilité. De nouveaux outils devront être mis en place, pour tenir compte d'un environnement très vivant (d'un point de vue technique et structurel) et des nouveaux besoins qui ne manqueront pas de naître. Pour assurer cette évolution il faudra continuer à se montrer très attentif au monde extérieur et très réactif. Comme les standards en matière d'IdM ne font qu'émerger, il sera important dans l'avenir de valider nos choix ou de les adapter en fonction des futures normalisations qui régiront tous les échanges d'information concernant authentification et autorisation.

L'intégration de l'infrastructure IdM de l'EPFL devra être faite avec les solutions extérieures.

Les systèmes d'information (SI) reposent sur l'IdM, une consolidation de l'infrastructure IdM milite donc en faveur d'une évolution vers une meilleure coordination et harmonisation des SI de l'EPFL.

8 Qualités de cette infrastructure

– Pérennité

La totalité des codes de ces outils est disponible sous forme source et plusieurs personnes peuvent en assurer la charge immédiatement. Les éditeurs de logiciels trépassent, mais les services informatiques demeurent.

- Souplesse d'évolution

L'environnement informatique est un des domaines qui évolue le plus vite. Il est fondamental de pouvoir réagir de manière très rapide devant les nouvelles situations qui se posent chaque jour. Avoir une équipe de personnes formées à tous les rouages du système est ici un avantage incomparable. Dans un futur assez proche, il va devenir nécessaire de gérer des personnes telles que les anciens étudiants ou des anciens employés. Le système devra évoluer pour faire face à ces nouveaux défis.

- Robustesse

Tout le système est pensé de manière à résister aux données erronées qui proviennent parfois des autres fournisseurs d'informations. Pour cela, des tests importants de cohérence sont effectués et il est toujours possible de revenir à la situation de la veille en cas de problème grave et nouveau.

- Réactivité

Si la robustesse n'a pas été suffisante (par exemple 3000 nouvelles accréditations d'étudiants arrivent à cause d'une erreur de date dans la base des étudiants ou le fichier journalier en provenance des ressources humaines a une structure incorrecte) la réaction doit pouvoir être immédiate. Là encore, une connaissance approfondie de tout le système est impérative.

- Modularité

Chaque outil fait peu, mais le fait bien. Les interfaces sont parfaitement définies : chaque module peut-être modifié, voire totalement remplacé dans la mesure où son interface ne change pas.

- Intégration

Chaque outil a été conçu pour s'intégrer à l'environnement aussi bien externe au service informatique (la multitude d'applications sécurisées faisant de l'IdM sans le savoir), qu'interne : l'utilisateur ne se rend même pas compte qu'avec une requête il fait appel à plusieurs systèmes sous-jacents.

- Coûts contrôlés

Le fait de disposer des sources de nos applications, d'être indépendant de tout éditeur de logiciels nous procure une maîtrise complète de l'outil informatique ; c'est fondamental dans le domaine de l'IdM mais ce n'est pas chiffrable.

9 Défauts

Le système a été développé en mettant l'accent sur la facilité de communication avec tous les SI de l'EPFL. En voulant satisfaire tous les besoins, nous avons parfois été obligés de mettre en place des structures trop complexes par rapport au problème réel tel qu'il aurait dû se poser. Un travail important qui reste à faire est la simplification des interfaces avec le SI. Ceci ne pourra se faire que par une meilleure coordination entre les acteurs du domaine.

10 Disponibilité de ces outils

Tous les outils utilisés ont été entièrement développés en interne à l'EPFL. La plupart sont relativement imbriqués dans le système d'information local et l'effort n'a pas été fait pour produire une version générique utilisable dans un autre contexte, bien que ce ne soit pas insurmontable. Seul ***Tequila*** est suffisamment générique et est déjà distribué en *open source.*

11 Conclusion

L'Identity Management est la clé du système d'information institutionnel. Sans un IdM fonctionnel, pas de partage efficace d'information et pas de sécurité dans les échanges. C'est un domaine stratégique qu'il convient de soigner et surtout dont il faut garder la maîtrise. Nous disposons d'une base solide sur laquelle nous pouvons construire un édifice utile à toute la communauté. Les priorités sont la consolidation, la généralisation à tous les SI de l'école et l'ouverture sur le monde extérieur.

Bibliographie

[1] http://accreditation.epfl.ch/, description du système d'accréditation.

[2] http://tequila.epfl.ch/, page principale ***Tequila.***

[3] http://ditwww.epfl.ch/publications-spip/spip.php?article996**,** Intégration ***Tequila Shibboleth***. Flash Informatique janvier 2006.

[4] http://ditwww.epfl.ch/publications-spip/spip.php?article680, Application ***Guests***. Flash Informatique 2004.

[5] http://www.switch.ch/

[6] http://www.switch.ch/aai/

[7] http:/shibboleth.internet2.edu/

[8] http://gaspar.epfl.ch/docs/gaspar2007.pdf

[9] http://slpc1.epfl.ch/public/KIS/AAI.pdf

[10] http://en.wikipedia.org/wiki/Public_key_infrastructure