La gestion des identités à l'École polytechnique Fédérale de Lausanne

Claude Lecommandeur

École Polytechnique Fédérale de Lausanne

Novembre 2007

Plan

- Gestion des identités.
- Beaucoup (trop) d'intervenants.
- Comment on faisait avant.
- Enjeu de l'IdM.
- Notre démarche.
- 2 outils mis en place à l'EPFL.
- Accred : rattachements, droits et rôles.
- Tequila : authentification et contrôle d'accès Web.
- Quelques pistes pour le futur.

Gestion des identités

- La question fondamentale auxquelles sont confrontées les applications sécurisées est : « Comment savoir si mes utilisateurs ont le droit d'utiliser mes services et lesquels ? »
- Si on veut proposer un outil central de soutien à ces applications, il va falloir répondre à la question fondamentale : « Qui a droit à quoi ? »
- Pour répondre correctement à cette question, il faut disposer d'une infrastructure informatique et d'un ensemble de processus administratifs complexes.
- C'est cette infrastructure et ces processus qu'on qualifie de « gestion des identités ».

Gestion des identités

- Offrir une vue uniformes des personnes en masquant les spécificités des applications sous-jacentes.
- Définir un modèle d'identité :
  - Qu'est ce qui est nécessaire et suffisant pour servir de support au contrôle d'accès.
  - Quelles relations entre les données des applications « natives » et les données du système d'IdM. Sémantique des attributs des personnes.
  - Parfois facile (nom, prénom, etc.), parfois difficile (statut, classe, etc.).

Beaucoup (trop) d'intervenants

- Ressources humaines : personnel contractuel.
- Service académique : étudiants.
- Incubateur d'entreprises : personnel des entreprises.
- Associations d'étudiants : alumni.
- Association du personnel : retraités.
- Localement dans les unités : stagiaires, professeurs invités, etc.
- Personne : d'autres cas.

Beaucoup (trop) d'intervenants

- Chaque fournisseur d'identité utilise ses propres outils et ses propres formats.
- La sémantique des attributs des personnes est mal définie car pas destinée à être utilisée dans un autre cadre.
- Beaucoup de données importantes ne sont pas gérées du tout : rôles, droits,..,
- Nécessité de disposer d'un cadre unificateur pour la gestion des identités.

Comment on faisait avant

- De plus en plus d'applications ont besoin d'un contrôle d'accès pour délivrer leurs services.
- L'ancienne méthode qui consistait à avoir une liste d'utilisateurs avec leurs droits à l'intérieur même de l'application n'est plus guère utilisable :
  - Liste rapidement obsolète.
  - Pas de partage des informations entre applications.
  - Accès malaisé aux données globales.
- Ça ne marche que pour un petit nombre d'utilisateurs.

Enjeu de l'IdM

- Disposer d'un cadre unifié et bien géré des identités permet :
  - Une meilleure protection des données personnelles : il n'est pas nécessaire de distribuer des fichiers de personnes à tout va juste pour créer des usernames ou des adresses email.
  - Une meilleure sécurité informatique : la liste des personnes autorisées est mise à jour en temps réel => pas de vieux usernames qui trainent sur des machines.
  - Toutes les applications sécurisées disposent de ces données fiables. Une fois passée la barrière psychologique de l'abandon de la gestion locale, une utilisation généralisée devient possible.
  - Tous les types de personnes sont gérés et de manière très dynamique : un professeur invité qui est là pour 2 semaines, peut disposer d'une identité et des accès nécessaires dans les minutes qui suivent son arrivée.

Démarche suivie à l'EPFL

- Modulaire : Les outils d'IdM sont conçus comme un ensemble ouvert de briques interconnectées. Chaque brique assure une fonctionnalité limitée, mais le fait bien.
- Pragmatique : Développement au fur et à mesure de l'évolution des besoins en essayant de garder un niveau d'abstraction d'avance.
- Prospective : Dans la mesure du possible, essayer d'anticiper les besoins futurs.
- Pour atteindre des objectifs, il est impératif de faire des développement souples pouvant être rapidement refactorisés.

Survol de 2 outils : Accred et Tequila

- Accred :
  - Gestion des rattachements, droits et rôles des personnes.
- Tequila :
  - Authentification et contrôle d'accès Web.

Accred

- Chaque personne peut avoir un ou plusieurs rattachements à des unités organisationnelles.
- Chaque personnes peut avoir un ou plusieurs droits ou rôles relativement à des unités.
- Les associations personne/droit/unité et personne/rôle/unité sont indépendantes des rattachements de le personne.
- A chaque rôle sont associés un certain nombre de droits. Une personne ayant ce rôle, a automatiquement les droits associés et peut aussi les déléguer.

Accred - Rattachements

- La personne fait partie de l'unité, le sens profond de ceci est libre.
- Les unités sont organisées en arbre. L'appartenance à une unité implique l'appartenance aux unités parentes.
- Attributs associés à un rattachement :
  - Statut : Personnel, Hôte, Hors-EPFL, Étudiant, Alumni, Retraité.
  - Classe : Professeur, Assistant, Secrétaire, ... (une dizaine).
  - Fonction : Une vaste liste.
  - Etc.

Accred - Rattachements

Accréditation | Propriétés | Historique

Accréditation de Claude Lecommandeur dans l'unité KIS

Nom	**Claude Lecommandeur**
Sciper	105640
Unité	**KIS**
Statut	Personnel
Classe	Personnel technique/administratif
Fonction	Adjoint scientifique
Date début	17 Jan 2004
Date fin	Illimité
Créateur	Vous-même
Date création	17 Jan 2004
Commentaire	
Auteur	Vous-même

Voulez-vous ? [Modifier cette accréditation] [La détruire]

Accred - Droits

- Généralement associés à des applications informatiques.
  - Commander des tickets de train, commander des logiciels, ...
- Création rapide et souple.
- Actuellement 24 droits définis à l'EPFL.

Accred - Droits

Droit	Unité (s)
Accès Réseau pour Hôtes	☒ DIT-DEV ⊞
Accès au serveur AFS	☒ DIT-DEV ☒ PL-DIT ⊞
Administration des comptes GASPAR	☒ KIS ⊞
Commandes en ligne économat	☒ KIS ⊞
Services Réseau EPNET	☒ DIT-DEV ⊞
	⊞

Accred - Rôles

- Peu nombreux, seulement au nombre de 6.
  - Responsable informatique.
  - Responsable communication.
  - Responsable administratif.
  - Responsable infrastructures.
  - Responsable sécurité.
  - Responsable accréditation.
- Haut niveau conceptuel.

Accred - Rôles

Rôle	Unité (s)
Responsable accréditation	☒ PL-DIT ☒ IN-DOC ⊞
Responsable administratif	☒ KIS ⊞
Responsable informatique	☒ PL-DIT ⊞
Responsable infrastructures	⊞

Gestion d'Accred

- Rôle « Responsable accréditation »
  - Donne les droits « Accréditation » et « Attribution de rôles »
- Droit « Accréditeur »
  - Gestion des rattachements.
- Droit « Attribution de rôles »
  - Gestion des rôles.
- Ça se gère tout seul.
- Création d'un réseau de personnes aux rôles bien définis.

Quelques chiffres

- Responsables accréditations : 390
  - Faculté : 36, Institut : 68, Labo : 273.
- Accréditeurs : 247
  - Faculté : 8, Institut : 54, Labo : 178.
- Responsables informatiques : 299
  - Faculté : 28, Institut : 61, Labo : 204.
- Responsables communications : 97
  - Faculté : 18, Institut : 16, Labo : 57
  -


T’es qui, là ?

Tequila

- Offrir ses services à toutes les applications sécurisées, indépendamment des OS et des langages.
- Communication avec d'autres infrastructures d'authentification (Shibboleth, etc.).
- Support du Single Sign-on.
- Support d'un modèle souple de coopération de serveurs (fédération, peer-to-peer).
- Contrôle par l'utilisateur de la divulgation des données le concernant.

Tequila : comment ça marche ?

- Étape 1 : L'utilisateur (**U**) essaye d'accéder à une page Web protégée.
- Étape 2 : L'application sécurisée (**A**) crée une requête sur le serveur Tequila (**T**) avec les contraintes désirées, en échange, celui-ci lui donne une clé.
- Étape 3 : **A** redirige **U** vers **T** avec la clé sus-mentionnée.
- Étape 4 : Si **U** est déjà authentifié auprès de **T**, on saute à l'étape 7.
- Étape 5 : **T** propose un écran de login à **U**, celui-ci s'authentifie.
- Étape 6 : **T** vérifie que l'authentification est correcte.

Tequila - comment ça marche ?

- Étape 7 : **T** vérifie que **U** satisfait aux contraintes demandées par **A**.
- Étape 8 : **T** redirige **U** vers **A** avec une autre clé dans ses bagages.
- Étape 9 : **A** lit cette clé, et demande à **T** si elle est correcte et quelles sont les données utilisateurs associées.
- Étape 10 : **A** est content, il connait les informations sur son utilisateur, il sait que celui-ci vérifie les contraintes nécessaire, **A** et **U** vont pouvoir faire un bout de chemin ensemble.

Tequila - contrôle d'accès

- Tequila connaît des utilisateurs. Chaque utilisateur possède un certain nombre d'attributs éventuellement multivalués. dont Tequila connaît la(les) valeur(s).
  - Mono-valués : Nom, Prénom, Salaire, ...
  - Multi-valués : Unité, Groupe, ...
- Les applications clientes peuvent demander à Tequila de vérifier que des contraintes sont satisfaites sur un ou plusieurs de ces attributs.
  - TequilaAllowIf prenom=claude
  - TequilaAllowIf groupe=aasl
  - ...

Tequila - contrôle d'accès

- Il est possible de mettre une expression portant sur plusieurs attributs.
- Les droits et rôles des personnes sont aussi testables.
- La valeur de l'attribut est la liste des unités où la personne possède ce droit.
  - TequilaAllowIf droit-distrilog
  - TequilaRequest droit-distrilog
  - TequilaAllowIf role-respadmin

Tequila - délégation

- Un serveur Tequila peut faire confiance à d'autres serveurs Tequila et leur déléguer l'authentification et le contrôle d'accès.
- Chaque serveur décide à qui il fait confiance.
- Tous les modèle de délégation de confiance sont possible : fédération, arborescence, deux à deux.

Tequila - Données personnelles

- Les données non « sensibles » sont données sans contrôle aux applications clientes.
- Les données sensibles ne sont données que sur accord de l'utilisateur. Soit au moment du login, soit une fois pour toute pour certaines applications clientes.
  - Je donne mon nom à tout le monde.
  - Je veux que l'on me pose la question quand on demande ma photo.
  - Je ne donne mon salaire qu'à l'application comptabilité.
- A tout moment, on peut demander au serveur ce qu'il connaît sur nous.

Tequila - Policies

Name	Value
name	Lecommandeur
firstname	Claude
statut	Personnel
classe	Personnel technique/administratif
email	claude.lecommandeur@epfl.ch
title	Adjoint scientifique
unit	Système d'information et de support à la connaissance, KIS
where	KIS/PL-DIT/PL/EPFL/CH
office	MA C1 652

Tequila - Policies

groupid	10077
group	APC, Camipro2, Clients_DIT_salles_serveurs, DIT, KISCO, PWAD, aasl, bureauaccred, cognac.admin, dit-projets, groupware, guests.admin, infoscience_ic, infoscience_users, myepfl-agenda-pilote, oscar2006, qwe, slb-ldap, slb-scoldap, slb-test-tequila
org	EPFL

Tequila - Policies

droit-msdnaa	DIT-DEV, DIT-EX, DIT-GE, DIT-PRO, DIT-SB, DIT-SUP, DIT-TI, KIS, PL-DIT, SB-IT, SSI
photo	

Tequila - Policies

Attribute 'photo' policy

Organization	Resource	Policy
EPFL	Bottin	Yes
	All others	Ask
ETHZ	All	No
UNIL	UNILres1	Yes
	All others	No

[Modify policy]

Tequila - Shibboleth

- Un serveur Tequila peut déléguer l'authentification à un serveur Shibboleth.
- Il se comporte comme un WAYF, permettant à l'utilisateur de choisir son serveur.
- Et comme un Service Provider : il demande au serveur Shibboleth la valeur des attributs pour la personne et vérifie lui-même les contraintes quand c'est possible, si les attributs délivrés par le serveur Shibboleth sont suffisamment riches.
- Table de « mapping » entre les attributs Tequila locaux et les attributs Shibboleth.

Tequila – Interface client.

- Modules clients en Perl, PHP, Java, Ruby, ASP pour les CGI.
- Exemple en Perl :

```
use Tequila::Client;
my $tequila = new Tequila::Client ();
$tequila->setservice   ("Tequila Perl Client test");
$tequila->allows       ("categorie=epfl-alumni");
$tequila->require      ("group=AASL");
$tequila->request      ("name",  "firstname", 'unit', "email", "title", "phone");
$tequila->authenticate ();

my     $org = $tequila->{org};
my    $user = $tequila->{user};
my    $host = $tequila->{host};
my     $key = $tequila->{key};
my $appargs = $tequila->{appargs};
```

Tequila – Interface client.

- Module Apache pour les documents statiques (ou CGI).
- Les données de configuration sont mises dans le fichier httpd.conf :

```
LoadModule tequila_module     /usr/lib/httpd/modules/mod_tequila.so

<IfModule mod_tequila.c>
  TequilaLogLevel       100
  TequilaLog            /etc/httpd/logs/tequila.log
  TequilaServer         tequila.epfl.ch
  TequilaSessionDir     /var/www/Tequila/Sessions
  TequilaSessionMax     3600
  TequilaCAFile         /etc/httpd/conf/ssl.crt/caepfl.crt
  TequilaCheckServerName
  </Location>
</IfModule>
```

Tequila – Interface client.

- Les données de spécifiques sont mises dans le .htaccess :

```
TequilaService "Page a acces controle"
TequilaAllows  categorie=Shibboleth
TequilaAllowIf droit-distrilog
TequilaAllowIf org=epfl&group=accreds
TequilaRequest uniqueid,username,email
```

Tequila

- Tequila offre une vision unifiée du système d'IdM sous-jacent.
  - Toutes les données passent par une liste d'attributs associés aux personnes.
  - Par exemple : avoir le droit « adminad » pour les unités KIS et DIT sera traduit par : la valeur de l'attribut « droit-adminad » est « KIS,DIT »
  - Faire partie du groupe « AASL » se traduira pas l'attribut « group », qui est une liste des noms de groupes auxquels appartient la personne, contiendra la valeur « AASL »
- Ce système uniforme permet à l'utilisateur gérant une application sécurisée de totalement ignorer cette structure sous-jacente.

Quelques pistes pour le futur

- Ouverture vers d'autres systèmes d'authentification : OpenID.
- Offrir des modèles plus souples d'IdM distribuée : au delà des fédérations.
- C'est l'utilisateur (application cliente) qui doit pouvoir décider qui il veut autoriser
  - Allows OpenID::url
  - Allows SomeProtocole::SomeOrg::Someone
- Mettre les contraintes de contrôle d'accès en un lieu centralisé (dans le serveur)
  - Meilleure visibilité et gestion des règles de fonctionnement du système d'information : « Business rules ».
  -

Conclusion

- Combinaison d’un ensemble d’outils et de processus.
- Pas de solutions miracles.
- Questions ?