
eGovernment-Symposium
Contrôle d'accès,
une approche self-service !
Concept et retour d'expérience
administration générale
service d'organisation et d'informatique
Lausanne

Présentations

administration générale
service d'organisation et d'informatique

Jean-Daniel SCHLAEPPY

jean-daniel.schlaeppy@lausanne.ch

Chef de la section Etudes et Applications

Pilotage du programme « CyberAdministration »

Pascal FONTAINE

pascal.fontaine@lausanne.ch

Chef de projet sécurité

IAM (Identity and Access Management)

CISSP, CISA,
CISM, LA27001

Lausanne

Agenda

1. Programme cyberadministration
2. Pourquoi une approche self-service ?
3. Pourquoi sur le contrôle d'accès ?
4. Principe de la « légitimation »
5. Démonstration
6. Retour d'expérience
7. Discussion

administration générale
service d'organisation et d'informatique

Lausanne

Programme cyberadministration

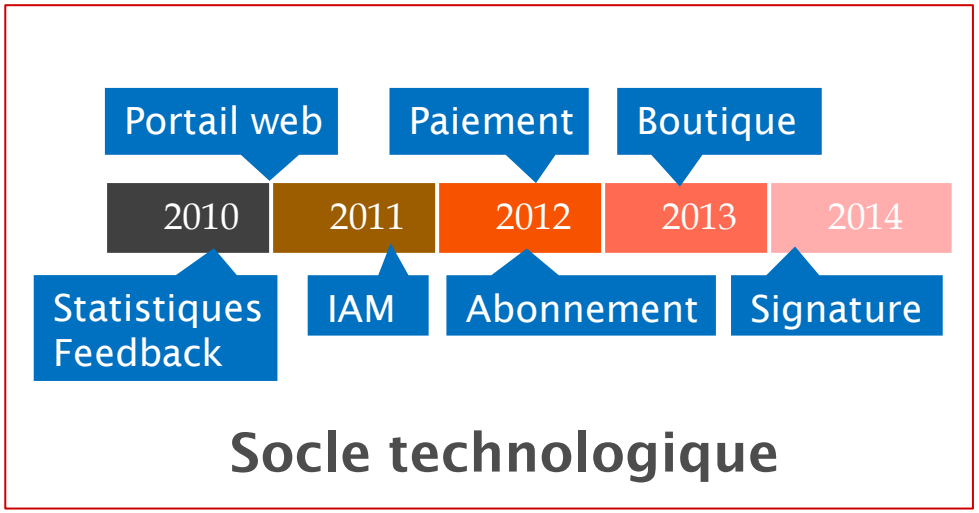
2006
Etude préalable

2009
Financement

11.2011
1er lot (SI)

04.2012
2ième lot (ASST)

09.2012
3ième lot (CH)



Lausanne

Objectifs de la cyberadministration

Objectifs de la Confédération

L'efficacité	· Favoriser le flux de l'information et de la communication
La transparence	· Donner accès à la bonne information et assurer la traçabilité
La souplesse	· Faciliter l'adaptation à un environnement en constante mutation
La participation	· Encourager la participation aux processus politiques et administratifs

Objectifs de la Ville

La transversalité	· Faciliter les échanges entre les services de l'administration
L'accessibilité	· Favoriser l'accessibilité de l'administration à tous les usagers, à tout moment et en tous lieux
L'attractivité	· Promouvoir l'attractivité de l'administration auprès de la population et des entreprises

Lausanne

Organisation de la cyberadministration

Gouvernance stratégique

COPILINF: Délégation municipale
3 municipaux et 5 chefs de services

Gouvernance du programme

Chef du programme:
Jean-Daniel Schläppy

- Comité « Droits et règlements »
- Comité « Paiement-encaissement »
- Comité « Communication »
- Comité « Accompagnement au changement »
- Comité « Données de références »
- Comité «Indicateurs et optimisation »

Gestion de projets

COPIL:
- Chefs de services
- Chefs de projet
- Chef du programme

COPROJ:
- Chefs de projet
- Représentants projet

Pourquoi une approche self-service ?

Approche « classique »

- Processus d'inscription complexe (identification formelle de la personne)
- Accès à la fin du processus
- Délégation difficile
- Adaptée à toutes les prestations
- Cycle de vie externe au processus métier

Approche « self-service »

- Processus d'inscription simple
- Accès immédiat
- Procuration simple
- Ne couvre pas tous les types de prestations
- Utilisation des processus métiers existants pour la gestion du cycle de vie

Ces deux approches sont complémentaires, l'une n'exclu pas l'autre !

Réconciliation des données…

Constat 1:

Il n'existe aucune « clé » permettant la réconciliation des données entres les différents domaines/métiers des administrations (protection des données oblige!)

Constat 2:

La fédération avec un IdP (p.e. SuisseID) ne fournit pas les données nécessaires et suffisantes pour lier le détenteur avec les données des domaines/métiers

Bilan:

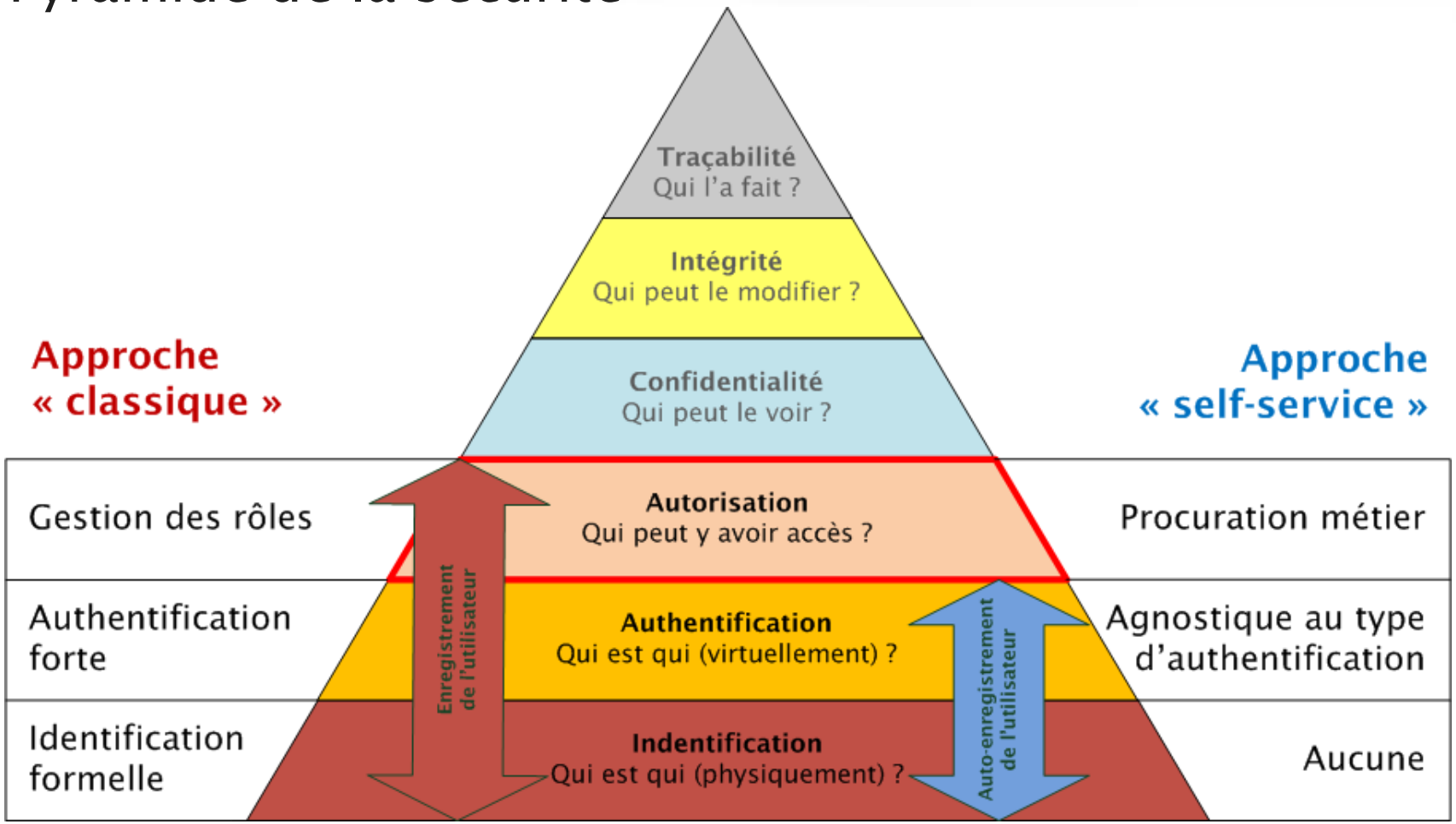
Une identification avec une authentification (même forte) ou une fédération ne permet pas de réconcilier les données personnelles pour plusieurs métiers

Besoin:

Développer une solution d'accès autour d'une procuration métier

Pourquoi sur le contrôle d'accès ?

Pyramide de la sécurité



Un peu de vocabulaire…

Procuration:

Document par lequel une personne donne le pouvoir à une autre d'agir en son nom

Usager:

Personne qui utilise un service public

Utilisateur:

Personne qui est définie dans le système d'information

Utilisateur légitimé:

Utilisateur qui est au bénéfice d'une procuration métier valable, en regard d'un usager

Procuration vs Rôle ?

La **procuration métier** est associée au **rôle « légitimé »**
qui se définit comme
« **représentant autorisé de l'usager** »

Approche « classique »

- Rôles gérés sur la base du profil de l'utilisateur/titulaire par l'administration

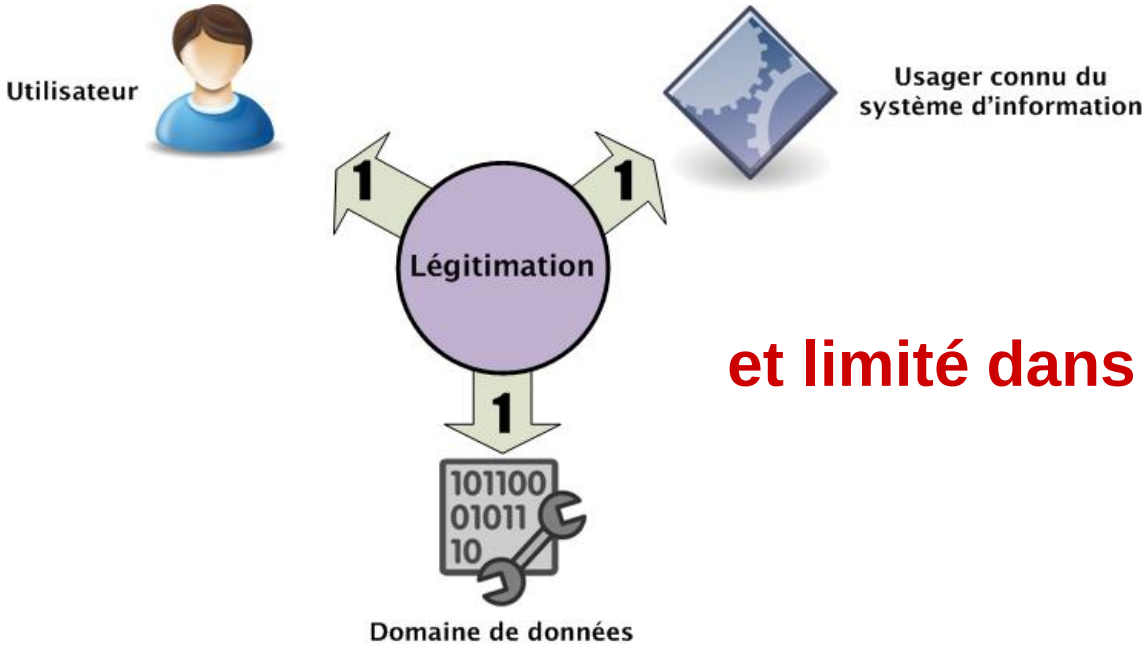
Approche « self-service »

- Rôles autogérés par l'usager via les procurations métier
- Révision implicite

*Uniquement avec la procuration/rôle légitimé, on **ne** peut **pas** faire la différence entre le titulaire (usager) et son délégué (utilisateur) !*

Principe de la légitimation

Réconciliation de l'**utilisateur** et d'un identifiant d'un **usager** sur la base d'un **secret** partagé.



et limité dans le temps!

On mémorise les légitimations d'un utilisateur afin qu'il ne doivent pas les refournir à chaque visite.

Le secret partagé

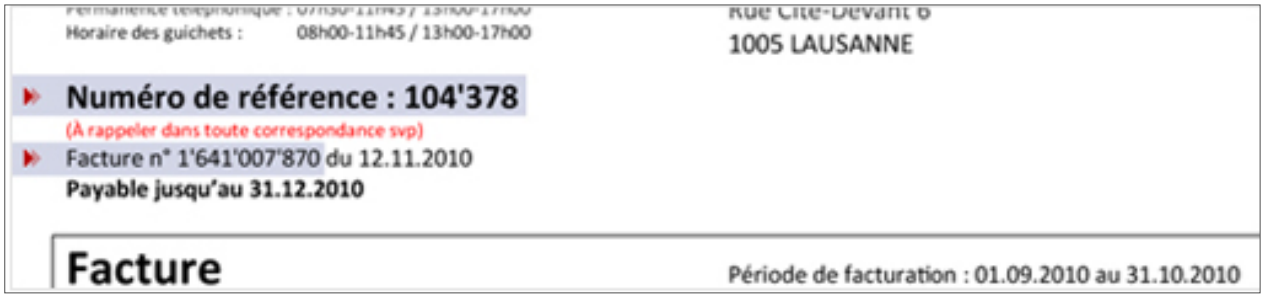
Le secret partagé doit être:

- relatif à un domaine/métier
- connu uniquement de l'usager et de l'administration
- aléatoires et non devinables

Procuration:

L'usager peut transmettre son secret en guise de procuration

Exemple:


Horaire des guichets : 08h00-11h45 / 13h00-17h00

1005 LAUSANNE

Numéro de référence : 104'378

(À rappeler dans toute correspondance svp)

Facture n° 1'641'007'870 du 12.11.2010

Payable jusqu'au 31.12.2010

Facture

Période de facturation : 01.09.2010 au 31.10.2010

Les états possibles de légitimation

Actif:

La légitimation est valide

Retiré

La légitimation a été retirée par l'utilisateur

Révoqué

La légitimation a été bloquée par un administrateur et ne peut plus être invoquée

Expiré

La légitimation a dépassé sa période de validité

Evolutions

Code uniques de légitimation

Dans certains cas, il n'existe pas de secret partagé issu du processus métier
L'objectif de cette extension est de permettre la création et l'acheminement d'un secret à l'utilisateur

Fédération

Avec le self-service, les usagers ne sont pas identifiés.
Cette situation ouvre naturellement la porte à la fédération (OAuth2, SAML2)

« Légitimation naturelle »

En identifiant formellement l'utilisateur **et** en lui mettant à disposition une solution d'authentification forte, on devient capable de l'associer avec les données du système d'information qui représentent l'usager.

Démonstrations

Consultation des données liées à une référence SI

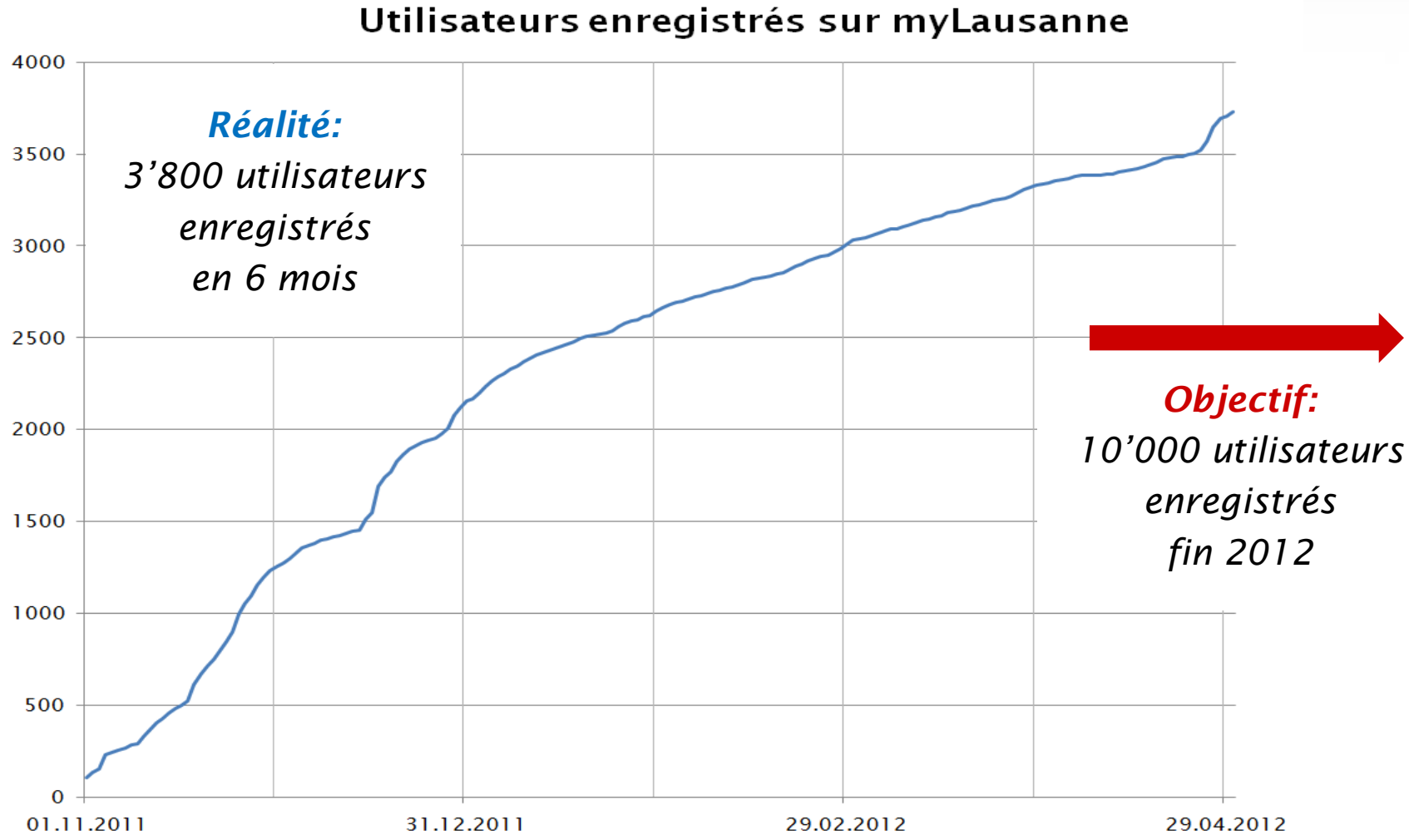
1. **Création d'un compte personnel**
   - Enregistrement self-service
   - Activation

2. **Accès au portail myLausanne**
   - Liste des prestations

3. **Légitimation SIL sur mes données**
   - Autorisation self-service

4. **Seconde légitimation SIL**
   - Simplicité de la procuration

Retour d'expérience



Retour sondage

Par comparaison à d'autres systèmes en ligne, et en fonction de la sécurité que vous jugez nécessaire, le processus d'enregistrement et de connexion est-il:

	Answer	Count	Percent	20% 40% 60% 80% 100%
1.	**Simple et rapide**	**19**	**54.29%**	
2.	Simple et sûr	7	20.00%	
3.	Complexe mais nécessaire	4	11.43%	
4.	Long et pénible	3	8.57%	
5.	Autre	2	5.71%	
	Total	**35**	**100%**	

Discussion


QUAND JE ME DIS QUE JE SUIS RELIÉ AU MONDE ENTIER
JE ME SENS TOUT PETIT
SI JE ME DIS QUE LE MONDE ENTIER EST RELIÉ À MOI
...ÇA VA UN PEU MIEUX
© casterman - geluck

Merci pour votre attention !