



CONFÉRENCE INTERCANTONALE
DE L'INSTRUCTION PUBLIQUE DE
LA SUISSE ROMANDE ET DU TESSIN

ACCÈS AUX RESSOURCES NUMÉRIQUES

Identification, authentification et
navigation entre les plateformes et
les portails officiels

Recommandations de la CORENE

Juin 2014



Contenu

Bref rappel du dossier	3
Objectif	3
A. Etat des lieux.....	4
1. Situation actuelle (sans identifiant unique)	4
2. Situation à terme (avec identifiant unique- SSO).....	5
3. Fédération d'identités	6
4. Choix technique	7
Shibboleth	7
B. Argumentaire détaillé	8
Pourquoi un identifiant unique ?.....	8
Pourquoi un accès sécurisé et différencié ?.....	8
Pourquoi une fédération d'identités ?.....	9
Educa.ch :.....	9
Quelles implications pour les partenaires commerciaux (éditeurs,...) ?	10
Conclusion	10
Proposition	10

Documents de référence

- Présentation Switch
- Présentation educa
- Etude principale J. Bieri "Participation du canton du Jura à une fédération d'identités autour d'educa.ID"
- Mandat CORENE, art2, al1.e.

Bref rappel du dossier

Conformément à l'Art.2, al.1 de son mandat, la CORENE s'est penchée sur les problèmes d'identification, d'authentification et de navigation entre les plateformes et portails officiels et a recherché des solutions qui permettent aux utilisateurs de tous les cantons d'accéder aux ressources partagées par d'autres cantons ou entités (PPER, BSN, ...). Ces solutions doivent également permettre d'accéder de la même manière aux futurs moyens commerciaux, négociés par la CIIP. Elle a mis en place un groupe de travail chargé d'évaluer la situation actuelle, de procéder à une étude de marché et de proposer des solutions.

Le groupe de travail a collaboré avec Monsieur J. Bieri pour aboutir à une analyse préliminaire qui a permis de dresser un état des lieux de la situation dans les cantons. Il a ensuite pris contact avec Educa.ch et Switch afin d'analyser les solutions proposées.

Il a pris connaissance de projets pilotes actuellement développés par Educa.ch avec le canton de Genève et la HEP BEJUNE (IdP et Service Provider) ainsi qu'avec la plateforme du PER (www.plandetudes.ch).

Le groupe de travail a présenté ses conclusions ainsi que ses propositions à la CORENE du 12 mars 2014.

Sur la base de ces propositions, la CORENE a procédé à une clarification des points importants dont la synthèse est intégrée dans le présent document.

Objectif

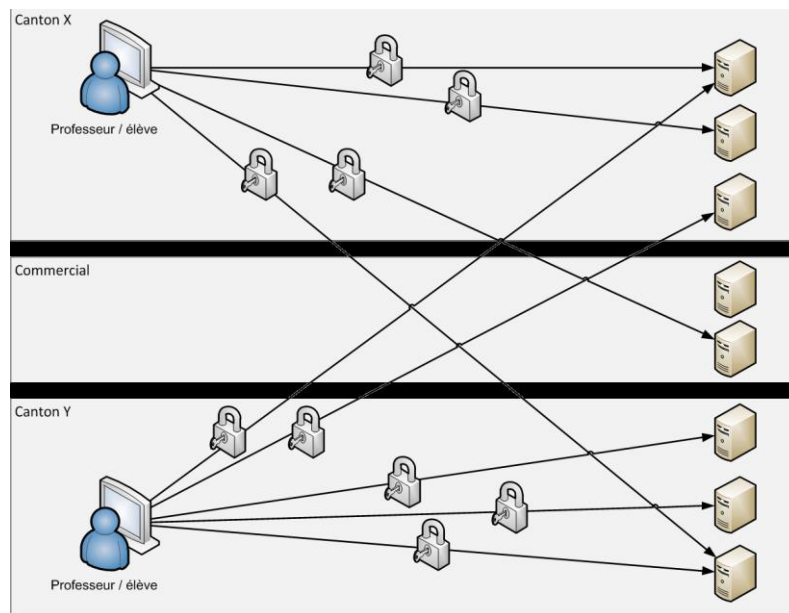
Offrir un accès individualisé, simple, efficace et sécurisé à des ressources électroniques d'enseignement et d'apprentissage (RéEA) de qualité en lien avec le Plan d'Etudes Romand (PER).

Les élèves, enseignants, futurs enseignants de tous les cantons doivent pouvoir accéder simplement au moyen d'un compte d'utilisateur unique aux ressources électroniques partagées par d'autres cantons ou entités (PPER, BSN, HEP,...).

A. Etat des lieux

Actuellement, lorsqu'un utilisateur souhaite se connecter à un portail cantonal ou à une plateforme, **il doit à chaque fois insérer un login et un mot de passe** puisque chaque portail-plateforme possède son propre système de connexion.

1. Situation actuelle (sans identifiant unique)



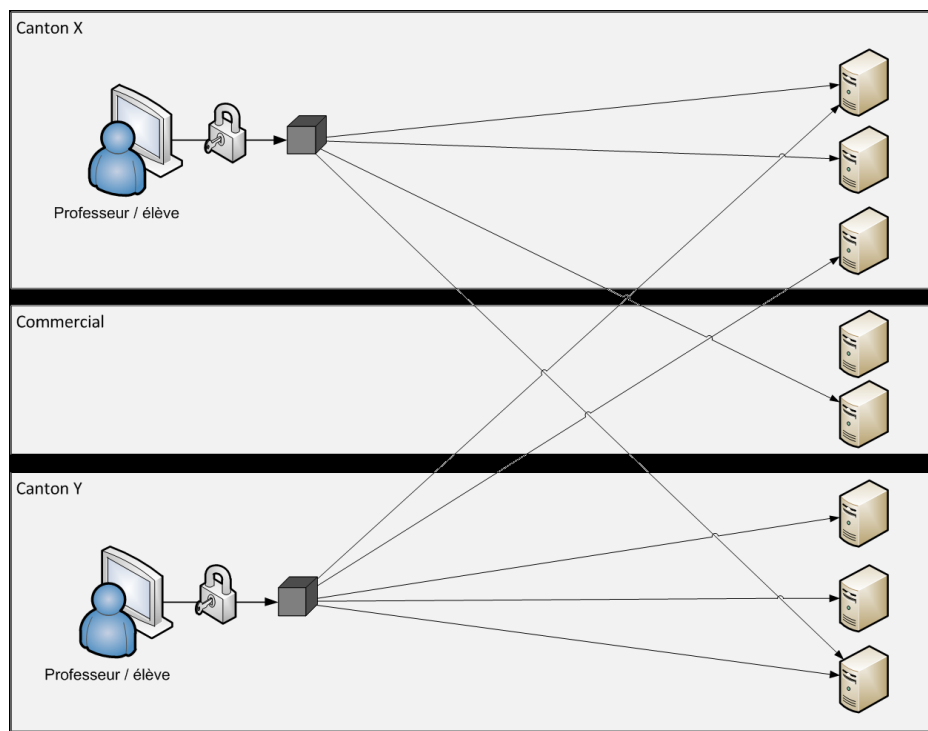
source : J.Bieri – Étude principale

Les ressources et applications ont été rédigées et développées par des développeurs différents (cantons, éditeurs,...) selon des standards variés et chaque application possède ainsi son propre système de connexion, situation qui multiplie les contraintes, tant pour l'utilisateur que pour le système.

Cette situation implique :

- La perte de maîtrise des données des élèves et enseignants par les cantons (protection des données).
- L'utilisation de plusieurs identifiants et mots de passe pour l'utilisateur (avec risque d'oubli).
- Une perte de temps à chaque connexion.
- Un système de sécurité pour chaque application/ressource en ligne.
- Un partage très compliqué des ressources.
- De multiples gestions des comptes dans chaque canton (impact financier).

2. Situation à terme (avec identifiant unique- SSO)



source : J.Bieri – Étude principale

Dans ce cas, l'utilisateur entre son login et mot de passe une seule fois et a directement accès à l'ensemble des ressources qui lui sont autorisées dans un environnement "fermé" et sécurisé.

La gestion de l'identité (logins et mots de passe) est maîtrisée par les cantons.

Cette configuration offre de nombreux avantages :

- Maîtrise par chaque canton de ses identités en conformité avec la législation sur la protection des données.
- Un seul login et mot de passe pour chaque utilisateur.
- Une fédération des systèmes d'authentification.
- Une sécurité accrue et une maintenance simplifiée.

3. Fédération d'identités

Sur la base de ces travaux, le groupe de travail a confirmé qu'une solution globale avec identifiant unique ne pouvait que passer par la création d'une **fédération d'identités**.

Chaque application/ressource possède un accès différent et donc sa propre clé. Il faudrait donc donner à chaque utilisateur un trousseau de clés lui donnant accès à toutes les ressources auxquelles il a droit. Pour éviter ce problème, il convient de mettre en place une fédération d'identités où chaque utilisateur reçoit, en fonction d'un profil déterminé, une seule clé lui donnant accès aux ressources auxquelles il a droit.

La mise en place d'une fédération d'identités implique :

- Un système de clé simple, unique, standardisé et sécurisé.
- La définition d'une série de caractéristiques non nominatives.

Ainsi, la fédération d'identités présente en particulier les avantages suivants :

- L'identification et l'authentification reste dans l'organisation – canton - de l'utilisateur (protection des données).
- Un seul compte à gérer pour l'utilisateur.
- Possibilité de partager entre cantons des ressources "protégées".
- Possibilité d'apporter une solution standardisée et reconnue au monde de l'édition, pour la version en ligne des ME.
- Pour les cantons, possibilité d'intégrer la fédération à tout moment.
- Réduction des coûts d'administration.

L'objectif premier de la fédération d'identités est de pouvoir partager des ressources ; toute ressource développée par un canton (ou un partenaire commercial) peut être diffusée à l'ensemble de la fédération.

La mise en place d'une fédération d'identités doit se construire autour d'un service central (educalD) qui fera le pont entre les utilisateurs, les fournisseurs d'identités et les fournisseurs de ressources. Le rôle de ce service se limite à guider les utilisateurs, aider les cantons à entrer dans la fédération, aider les fournisseurs de services (cantons, éditeurs commerciaux, CIIP) à se greffer sur la fédération.

4. Choix technique

Shibboleth

Le groupe de travail propose d'utiliser Shibboleth, standard basé sur la norme SAML2, un mécanisme de propagation des identités développé par la communauté Opensource Internet2 qui regroupe près de 200 universités aux USA et en Europe.

En Suisse, ce mécanisme, mis en place par SWITCH, fonctionne avec succès depuis 2003 dans les universités et certaines HEP. Il est déjà utilisé et maîtrisé par Educa.ch pour educaID dans les projets pilotes menés avec le canton de Genève et la HEP BEJUNE ainsi que par la plateforme du PER (www.plandetudes.ch/).

B. Argumentaire détaillé

Pourquoi un identifiant unique ?

- Différents publics avec différents avantages.
- Les enseignants et les élèves peuvent ainsi se concentrer sur l'utilisation pédagogique des ressources et non sur des considérations plus techniques.
- Pour les utilisateurs du système d'information, facilité d'utilisation (un seul compte à gérer) et facilité d'accès (un compte donne accès à tout). Pour les gestionnaires du système d'information : gestion uniforme et standardisée des comptes. Pour les autorités : maîtrise des données personnelles échangées, indépendance vis-à-vis des marques (publicité), maîtrise du monitoring de l'utilisation des ressources acquises auprès de tiers, refacturation possible.
- Une sécurité augmentée.
- A terme la situation actuelle deviendra ingérable, onéreuse et contre-productive.
- Gain de temps pour les enseignants et les élèves.

En résumé:

Afin de rationaliser la gestion du système d'information scolaire, promouvoir l'usage des technologies et favoriser le partage de ressources dans le respect de la législation, il convient de simplifier et d'unifier les accès par la mise en place d'une authentification unique (SSO), basée de préférence sur un annuaire central et cantonal.

Pourquoi un accès sécurisé et différencié ?

- Droits d'auteurs négociés au niveau national, intercantonal, cantonal, voire local, etc.
- Suivi pédagogique du travail des élèves (dans l'utilisation d'applications ou plateformes pédagogiques).
- Pour partager des documents avec un autre enseignant ou les élèves de sa classe.
- Obligation d'un accès différencié à des documents destinés à différents publics cibles.
- Licences d'utilisation : respecter le modèle économique des éditeurs de ME.
- Assurer la protection et l'intégrité des données.
- Assurer les spécificités de la pédagogie spécialisée.

En résumé :

- ***répondre à des impératifs de sécurité (protection des données, droits d'auteurs, intégrité des données, contrats de licence...);***
- ***permettre un accès personnalisé à des ressources adaptées et/ou spécifiques, en fonction d'attributs utilisateur (profils utilisateur, ayants droits);***
- ***assurer la traçabilité et le suivi des parcours utilisateur.***

Pourquoi une fédération d'identités ?

- Elle permet à chaque canton et à chaque fournisseur de ressources de rentrer dans le système quand il est prêt et de fournir d'un seul coup un accès à ses élèves et enseignants à toutes les ressources inscrites dans la fédération.
- Accéder avec un unique compte aux ressources en ligne, de plus en plus souvent intercantionales.

En résumé :

La fédération d'identités, de par sa gestion plus souple et modulaire, nous semble plus à même de tenir compte de la diversité des acteurs habilités (et reconnus par un office – p.ex.) à bénéficier de prestations numériques.

Educa.ch :

Concernant l'identification unique il est important de souligner le mandat d'educa.ch dans ce domaine. Educa.ch confirme qu'il y a non seulement l'obligation de contribuer à une fédération ID, mais aussi la volonté.

Des projets pilotes avec Genève et la HEP BeJuNe (IdP et Service Provider) sont en cours et avancent de manière très positive. educa.ch confirme que la solution technique est souvent plus facile à trouver que de se mettre d'accord sur le projet au niveau 'politique' : Ça commence avec l'identification de toutes les parties prenantes (auprès les cantons sont souvent plusieurs départements concernés) et mène jusqu'à la question du choix des attributs qu'on aimerait accoler à l'id.

- Tant qu'il s'agit de piloter des projets en bilatéral avec un partenaire educa.ch est capable de fournir les efforts nécessaires mais educa.ch tient à souligner la limite définie par sa planification annuelle : Elle définit des budgets pour tous les activités d'educa.ch.
- Le budget pour educa.ID sera éventuellement à revoir si tous les cantons romands voudraient commencer à développer un système d'identifiant unique en collaboration avec educa.ch.
- Dès qu'il s'agira de développer une fédération educa.ch aura à faire simultanément avec plusieurs partenaires. Il faudra trouver une organisation et des processus aptes à cette situation pour pouvoir assurer la gouvernance du système.

Le succès de la fédération dépendra d'une attribution adéquate et claire des responsabilités des participants à la fédération. Pour cela les cantons auront à se mettre d'accord, mais aussi le rôle de la CIIP et la fonction de la CORENE sera à évaluer et à définir.

Michael Deichmann, le responsable d'educa.ID prévoit d'organiser une première rencontre au niveau suisse dévolue à ce processus en automne 2014. Les membres de la CORENE et la CIIP y seront invités.

Quelles implications pour les partenaires commerciaux (éditeurs,...) ?

- Critères éliminatoires dans un appel d'offres public.
- Adaptation du produit.
- Devenir partenaires de la fédération.
- Ne traitent plus les données personnelles des utilisateurs.

Conclusion

Au terme de ses travaux, la CORENE estime qu'il est impératif de mettre en place rapidement une solution unifiée pour résoudre les problèmes d'identification, d'authentification et de navigation entre les plateformes et portails officiels.

La CORENE estime qu'il est indispensable de proposer un système standardisé simple, fiable, sécurisé et adaptable pour permettre à chaque canton d'avancer à son rythme, tout en assurant à terme une compatibilité supracantonale.

Elle souligne que la mise en place d'une fédération d'identités est une nécessité si l'on veut envisager la mise en commun des ressources disponibles.

A terme, tous les partenaires et toutes les instances impliqués dans l'Instruction publique pourront rejoindre cette fédération (cantons, HEP, etc).

Proposition

La CORENE demande l'ouverture d'un chantier concernant l'accès simplifié et sécurisé aux ressources numériques en collaboration avec tous les cantons, la CIIP et Educa.ch.

Il s'agira notamment de :

- Mettre en place des serveurs cantonaux d'identités, afin de préserver la maîtrise de chaque canton sur les données utilisateurs.
- Mettre en relation les serveurs d'identités cantonaux au moyen d'une fédération utilisant des normes et standards reconnus.
- Mandater une entité externe - Educa.ch - pour assurer la mise en œuvre technique et organisationnelle du projet.
- Définir clairement les responsabilités de chaque partenaire.
- D'évaluer les ressources humaines et financières nécessaires