

Groupe de travail AAS

Compte rendu de la première réunion du 10 avril 2003

Ministère délégué à la recherche

Projet : **Etablissement des recommandations en terme de** **Authentification – Autorisation – SSO** **dans le cadre du schéma directeur SDET**

| | |
|-------------------|---|
| À : | Jean-Michel BAUDEQUIN ; Nicolas CHUNG |
| De : | Jacques PANTIN ; Sébastien FRANCOIS |
| Présents : | Groupe AAS (sauf R. Vatré, E. Ferrari, C. Mathieu) DICTAO (J. Pantin, S. Francois) |
| Date : | 10 avril 2004 |
| Lieu : | 25, rue de la montagne Sainte Geneviève, Paris 5 ^{ème} arr. |
| Objet : | Première réunion du groupe de travail AAS |

La démarche d'analyse des problématiques AAS

La démarche, retenue par le groupe de travail AAS, s'organise autour de 3 grands axes d'analyse :

- **Identification / Authentification**
 - Définir la typologie des utilisateurs :
 - Quelles sont les familles d'utilisateurs référencés dans l'annuaire ?
 - Caractériser l'identifiant
 - Quel format d'identifiant adopter ?
 - Faut-il proposer un format d'identifiant universel ou un format adapté aux pratiques de chaque établissement qui puisse être reconnu par tous les environnements de travail ?
 - Les utilisateurs disposeront-ils d'un seul mot de passe pour accéder à l'ensemble des applications et des ressources ou de plusieurs mots de passe dont la complexité dépendra de l'application ?
 - Est-il stocké en local (dans la base applicative ou dans l'annuaire de l'établissement) ou en central dans l'annuaire national de l'éducation nationale ?
 - L'identifiant doit-il être caché ou peut-il être visible sur l'annuaire « page blanche » de l'établissement ou au niveau national
 - Comment construire l'identifiant ? A partir de l'adresse email ? En ajoutant la référence de l'établissement en préfixe ?
 - Quel est à longueur de l'identifiant ? Fixe ? Avec un delta (à définir) ?
 - Comment sont gérées les homonymies ? Ajout d'un chiffre d'indentation ?
 - Prévoit-on l'utilisation d'alias pour construire les identifiants ?
 - Définir les stratégies d'authentification
 - Quels sont les niveaux d'authentification à envisager (en fonction de la criticité des applications) ?
 - Doit-on distinguer plusieurs niveaux d'authentification pour les utilisateurs accédant à des applications sensibles ?
 - Quelles applications justifient une approche « IGC » à base de certificats électroniques ?
 - Comment positionner les « token » USB qui commencent à être utilisés dans le cadre de l'accès à des applications ou des ressources sensibles ?
 - Faut-il stocker le mot de passe dans l'annuaire ou le conserver au niveau des applications ?

 - Doit-on traiter l'authentification de manière centrale (au niveau inter établissement) ou locale (au niveau de chaque établissement) ?
 - Quels sont les services qui seront intégrés dans le cercle de confiance établissement ?
- **Gestion des identités et des droits**
 - Définir où les droits seront gérés
 - Au niveau de l'application ?
 - Au niveau de l'annuaire de l'établissement ?
 - Au niveau inter établissement
 - Définir les concepts associés aux droits applicatifs, aux profils, aux rôles et aux attributs

- **Propagation des attributs des utilisateurs**
 - Fédérer les identités des utilisateurs (Passport / Liberty Alliance) ?
 - Faire interagir les identités Passport et Liberty Alliance ?
 - S'assurer qu'il est possible d'intégrer les applications traditionnelles au système SSO ?

Objectifs des prochaines phases

Phase 2 : Etat des lieux et formalisation des projets en cours et des besoins fonctionnels cibles

Objectifs :

Il s'agira pour cette phase de :

- Synthétiser l'état des projets et des expériences sur le domaine AAS des membres du groupe
- Décrire les solutions installées et les projets en cours pour l'enseignement scolaire et supérieur :
 - Périmètre couvert
 - Modalités et pertinence des solutions retenues
 - Durée et coût de mise en œuvre de la solution
 - Difficultés rencontrées
 - Facteurs de succès
 - Risques identifiés
 - Possibilité de généraliser l'expérimentation
- Construire une typologie des utilisateurs
- Référencer les applications et les ressources en fonction de leur degré de criticité
- Caractériser un « point de fuite »
- Vérifier la compatibilité des solutions AAS avec les solutions d'annuaire ayant été retenues sur le projet AAS

Actions fixées :

Nous avons convenu au cours de la réunion du 10/04 la séquence suivante :

| Action | En charge |
|---|------------------------|
| Envoi des documentations décrivant les architectures et les mécanismes existants en termes de AAS | Groupe AAS |
| Entretiens avec les membres du groupe de travail : <ul style="list-style-type: none"> • Caractérisation des problématiques spécifiques aux établissements de l'enseignement scolaire et supérieur • Rappel des objectifs attendus par les membres du groupe (Pour chacun des 4 grands projets, un interlocuteur principal sera désigné comme contact pour les interviews menées par DICTAO) | Groupe AAS / DICTAO |
| Synthèse des points clés des systèmes existants et des besoins fonctionnels dans le domaine AAS | DICTAO |
| Formalisation des notions d'identification, d'authentification, de gestion des droits et de propagation des attributs | DICTAO |
| Construction d'un glossaire du vocabulaire utilisé dans le cadre de l'étude | Groupe AAS / DICTAO |

Ces actions s'étaleront du 11 au 31 avril 2003. La préparation de la prochaine réunion du groupe de travail, planifiée le 07 mai 2003, devra être finalisée le 05 mai 2003.

Phase 3 : Etablissement des scénarios possibles et choix du scénario cible

Objectifs :

Il s'agira pour cette phase de :

- a) Elaborer plusieurs scénarios de mise en œuvre, en s'appuyant sur les résultats des travaux précédents (synthèse de l'expression de besoin et analyse de l'état de l'art)

Nous caractériserons chacun de ces scénarios en termes de :

- Processus concernés
 - Internes aux établissements
 - Faisant intervenir plusieurs établissements
- Système d'information
 - Processus d'enregistrement de l'utilisateur dans l'annuaire (à valider avec le groupe de travail annuaire)
 - Homogénéisation des processus d'authentification et d'identification des usagers entre les différents établissements en reposant sur les standards (Liberty Alliance, Microsoft Passport)
- Infrastructure technique
 - Schéma d'architecture retenu
 - Outils et solutions
 - Standards utilisés
 - Stabilité, pérennité et potentiel d'évolution
 - Coûts de mise en œuvre
 - ...

Nous insisterons, dans la construction de ces scénarios, sur le besoin d'avoir une approche très progressive.

Pour des raisons de faisabilité, nous nous limiterons à 2 ou 3 grands scénarios. Nous nous laisserons, néanmoins, le droit de bâtir pour chacun d'eux, des variantes sur chacun des 3 postes (processus, système d'information, infrastructure technique).

Il est très important de noter que les solutions proposées ne devront pas remettre en cause les principes d'architecture du système d'information qui auraient déjà été retenus dans le cadre du projet annuaire.

- b) Choisir un scénario cible en :

- Identifiant et en caractérisant les critères d'analyse des différents scénarios identifiés
- Mettant en place une procédure d'évaluation
- Classant les différents scénarios
- Faisant valider par le groupe de travail une proposition cible

Actions fixées :

A définir à la fin de la phase précédente.

Phase 4 : Etablissement du plan d'actions majeures du scénario retenu

Objectifs :

Cette phase doit permettre de :

- Définir le plan d'actions majeures du scénario retenu présentant :

Les grandes étapes logiques de mise en œuvre, avec pour chacune d'elles (périmètre fonctionnel cible, acteurs concernés, types de technologies mises en œuvre)

Les grandes actions nécessaires

- Les objectifs de l'étape
- Les pré-requis, les acteurs impliqués
- Les technologies
- Les moyens nécessaires
- Les budget associés (dans une 'évaluation à grosses mailles')
- La stratégie de mise en œuvre
- Les risques associés
- Les produits de chaque étape

On ne se limitera pas à la dimension technique, mais on s'intéressera à l'ensemble des actions nécessaires au succès du projet :

- Dimension humaine
- Dimension organisationnelle
- Dimension réglementaire
- ...
- Discuter de ce plan d'actions et le faire valider par le groupe de travail

Actions fixées :

A définir à la fin de la phase précédente.

Planning des réunions de travail

Les dates fixées au cours de la première réunion de travail du 10 avril 2003 sont :

| Action | Date |
|---|--------------------------|
| 1 ^{ère} validation des résultats de la phase 2 <i>(Etat des lieux et formalisation des projets en cours et des besoins fonctionnels cibles)</i> | Mercredi 07 mai 2003 |
| 1 ^{ère} validation des résultats de la phase 3 <i>(Etablissement des scénarios possibles et choix du scénario cible)</i> | Jeudi 05 juin 2003 |
| 1 ^{ère} validation des résultats de la phase 4 <i>(Etablissement du plan d'actions majeures du scénario retenu)</i> | Mercredi 02 juillet 2003 |