Projet : schéma directeur des espaces numériques de travail (SDET)

Date : 10/07/2003

Type : dossier de recommandations

Version - Révision : **1.0**

RECOMMANDATIONS POUR LA GESTION DE L'AUTHENTIFICATION-AUTORISATION-SSO : AAS

Référence : AAS-V10

Numéro de la dernière page : 20

ETAT DU DOCUMENT

Révision	Désignation des modifications
1.0	Version initiale

Sommaire

1. Objectifs et enjeux

1.1. Contexte

Le « schéma directeur des espaces numériques de travail » fournit des recommandations sur les plans fonctionnel, organisationnel et technologique pour la mise en œuvre d'espaces numériques de travail dans les établissements d'enseignement.

Sur le plan technologique, en plus des orientations générales, trois thèmes (sous forme de volets indépendants du document principal) sont traités en priorité pour permettre l'interopérabilité des dispositifs déployés :

- volet 1 : les annuaires (LDAP) ;
- volet 2 : l'identification, l'authentification, la gestion des autorisations et du Single Sign-On (AAS) ;
- volet 3 : l'interopérabilité applicative.

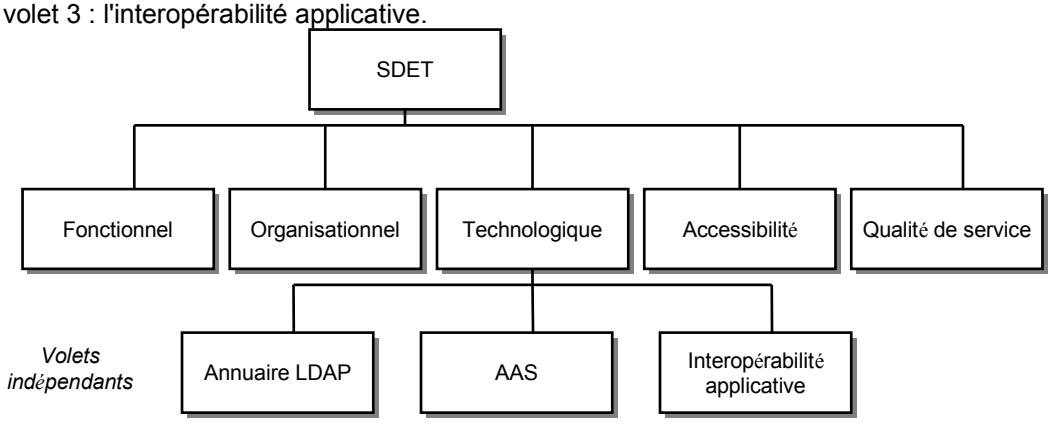

Figure 1 : organisation du SDET

Ce document est le volet du « schéma directeur des espaces numériques de travail » consacré au second point mentionné ci-dessus.

Ces recommandations s'adressent principalement aux responsables de projets de développement d'espaces numériques de travail et aux fournisseurs de services numériques accessibles à travers les ENT (en particulier les éditeurs de contenus).

1.2. Organisation et calendrier

Ce document est élaboré dans le cadre du SDET par un groupe de travail composé d'experts techniques de la communauté de l'enseignement scolaire et de l'enseignement supérieur.

Ce groupe de travail est piloté par la SDTICE, qui est en charge de l'élaboration du SDET. La SDTICE a fait appel à la société Dictao pour renforcer l'expertise technique du groupe et assurer l'assistance à maîtrise d'ouvrage. Dictao a en outre en charge la rédaction de ce document.

Les étapes de rédaction sont les suivantes :

- rédaction par le groupe de travail AAS de la version 1.0 (voir constitution paragraphe 8 page 20) ;

- appel à commentaires auprès de la communauté de l'enseignement scolaire et de l'enseignement supérieur portant sur la version 1.0 ;
- validation par le comité de pilotage du schéma directeur des espaces numériques de travail.

Une version 1.0 de ces recommandations est publiée courant juillet 2003. Le groupe AAS continuera son activité pendant l'année scolaire 2003-2004 afin de mettre, le cas échéant, en conformité ces recommandations avec les retours d'implémentations effectuées dans le cadre de l'appel à projets « espaces numériques de travail » (ENT) pour le scolaire et des Campus numériques volet 2 pour le supérieur.

1.2.1.Objectifs du groupe AAS

L'objectif premier est de fournir des préconisations en matière d'AAS qui permettront l'interopérabilité au sein des ENT, c'est-à-dire entre le socle de l'ENT (voir SDET, recommandations technologiques) et les services numériques proposés, qu'ils soient internes ou externes à l'établissement.

Du point de vue de l'usager, l'objectif est d'accéder, de manière simple, à l'ensemble des services numériques auquel il a droit, de façon sécurisée, dans le respect de sa vie privée et en n'ayant à s'authentifier qu'une seule fois.

Ces préconisations permettront à terme aux fournisseurs de services de proposer une interface AAS unique pour la communauté éducative, quels que soient l'établissement et la solution d'ENT utilisée.

Il conviendra donc de respecter ces préconisations, tant au niveau du développement de plates-formes d'ENT que de services numériques accessibles à travers les ENT.

Ce document fournit aussi des conseils (bonnes pratiques) en matière d'AAS résultant de l'expérience du groupe de travail dans ce domaine mais dont l'impact sur l'interopérabilité ne rend pas indispensable le respect.

Un document annexe complète ces recommandations dans le but de fournir les cadres de référence fonctionnel et technique ainsi que des scénarios de mise en œuvre. Le document désigné est l'annexe « Cadre de référence fonctionnel et technique ».

1.2.2.Niveaux de préconisations

Ce document décrira un certain nombre de préconisations et de conseils (bonnes pratiques). Afin de déterminer le niveau d'obligation de respect de ces préconisations, nous utiliserons la terminologie définie dans le RFC 2119 avec les traductions suivantes :

- MUST, SHALL : DOIT
- MUST NOT, SHALL NOT : NE DOIT PAS
- REQUIRED : EXIGE
- SHOULD : DEVRAIT
- SHOULD NOT : NE DEVRAIT PAS
- RECOMMENDED : RECOMMANDE
- MAY : PEUT
- OPTIONAL : FACULTATIF

Voici une traduction de la définition de ces termes dans le RFC 2119 :

1. DOIT : ce mot, ou le terme "EXIGÉ", signifie que la définition est une exigence absolue de la spécification.

2. NE DOIT PAS : cette expression signifie que la définition est une prohibition absolue de la spécification.

3. DEVRAIT : ce mot, ou l'adjectif "RECOMMANDÉ", signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer cet item particulier, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.

4. NE DEVRAIT PAS : cette expression, ou l'expression "NON RECOMMANDÉ", signifient que la définition est prohibée. Il peut toutefois exister des raisons valables, dans des circonstances particulières, quand le comportement particulier est acceptable ou même utile, de ne pas suivre cette recommandation. Mais les conséquences doivent être comprises et le cas soigneusement pesé.

5. PEUT : ce mot, ou l'adjectif "FACULTATIF", signifie qu'un item est vraiment facultatif. Un vendeur peut inclure l'item parce qu'un marché particulier l'exige ou parce qu'il estime qu'il améliore le produit tandis qu'un autre vendeur peut omettre le même item.

2. Documents de référence et terminologie

2.1. Documents de référence

Nom court	Nom complet	Description	URL
	Cadres de référence fonctionnel et technique	Etat de l'art en matière d'AAS	http://www.educnet.education.fr/ent
Liberty Alliance	Projet Liberty Alliance	Spécifications du projet Liberty Alliance (phase 1 finalisée et phase 2 en cours d'élaboration)	http://www.projectliberty.org
SAML	Security Assertion Markup Language	Spécifications OASIS de SAML	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
SDET	Schéma directeur des espaces numériques de travail		http://www.educnet.education.fr/ent
SUPANN	Annuaire de l'enseignement supérieur	Schéma d'annuaire pour l'enseignement supérieur	http://www.educnet.education.fr/ent
Shibboleth		Spécifications du projet Shibboleth (Internet 2)	http://shibboleth.internet2.edu
TERENA TF-AACE	Task force Authentication, Authorisation Coordination for Europe	Comparatif architectures d'authentification et autorisation.	http://www.terena.nl/tech/task-forces/tf-aace/temp/TF-AACE-B1-v6.pdf)
XACML	eXtensible Access Control Markup Language	SpécificationsSpecifications OASIS de XACML	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

2.1.1. Sigles et abréviations

Sigle - abréviation	Définition
AAS	Authentification - autorisation - SSO
AMUE	Agence de mutualisation des universités (http://www.cpu.fr/Amue/)
CRU	Comité réseau des universités (http://www.cru.fr)
DT	Direction de la technologie, ministère de la jeunesse, de l'éducation nationale et de la recherche
ENT	Espaces numériques de travail
FOAD	Formation ouverte et à distance
IGC	Infrastructure de gestion de clés publiques
LDAP	Lightweight Directory Access Protocol
OASIS	Organization for the Advancement of Structured Standards (http://www.oasis-open.org)
OTP	One Time Password
PDA	Personal Digital Assistant (équivalent français : assistant numérique personnel)

PKI	Public Key Infrastructure (équivalent français : infrastructure de gestion de clés publiques)
SAML	Security Assertion Markup Language
SDET	Schéma directeur des espaces numériques de travail
SDTICE	Sous-direction (de la DT) des technologies de l'information et de la communication pour l'éducation (http://www.educnet.education.fr)
SI	Système d'information
SOAP	Simple Object Access Protocole
SSO	Single Sign-On (équivalent français : authentification unique)
TERENA	Trans European Research and Education Networking Association (http://www.terena.nl/)
USB	Universal Serial Bus

2.1.2.Glossaire des termes employés

Terme	Définition
Assertion SAML	Message produit par une autorité SAML permettant, soit d'affirmer l'authentification d'une entité (utilisateur par exemple), soit de transmettre les attributs d'une entité ou les permissions d'authentification appliquées à une entité en respectant la politique de l'autorité.
Authentification	Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine des messages transitant par un réseau informatique. **L'identification permet de communiquer l'identité, l'authentification permet de la vérifier.** Les principaux moyens d'authentification sont : • mot de passe ; • clé symétrique ; • certificat ; • biométrie.
Authentification unique (ou Single Sign-On)	Concept consistant à permettre à un utilisateur d'accéder à des services numériques différents en ne devant s'authentifier qu'une seule et unique fois.
Autorisation	Mécanisme qui, a partir d'attributs, accorde ou non l'accès à un utilisateur, à des applications, fonctions ou données spécifiques.
Biométrie	Analyse mathématique des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable.
Campus numérique	Un Campus numérique se définit comme un dispositif de formation centré sur l'apprenant proposant des services innovants via des technologies numériques. Les ministères de l'éducation nationale et de la recherche ont lancé successivement, en 2000, 2001 et 2002, trois appels à projets pour la constitution de « Campus numériques français ». L'objectif majeur des appels à projets est d'arriver à construire une offre nationale de formation ouverte et à distance (FOAD) de qualité et compétitive sur le marché international. En 2002, l'appel à projets Campus numérique comportait un second volet concernant le développement technologique de solutions d'espaces numériques de travail.
Clé USB (ou token USB)	Clé matérielle, connectée par le port USB, permettant de stocker un certificat ou des données d'identification et éventuellement d'effectuer des opérations cryptographiques (chiffrement et signature par exemple).

Terme	Définition
Client réseau	Application logicielle de consultation et de traitement du contenu des pages Web accessibles à l'utilisateur. Par exemple : un navigateur Web tel que Netscape ou Internet Explorer ou une interface WAP.
Communauté de confiance	Ensemble d'utilisateurs rattachés à un ou plusieurs fournisseurs d'identités
Établissement	On appellera dans ce document « établissement » les structures du ministère de l'Éducation nationale comme les écoles, collèges, lycées, écoles d'ingénieur, universités, etc.
Espaces numériques de travail	Un espace numérique de travail désigne un dispositif global fournissant à un usager un point d'accès à travers les réseaux à l'ensemble des ressources et des services numériques en rapport avec son activité. Il est un point d'entrée pour accéder au système d'information de l'établissement.
Fournisseur d'identités	Entité responsable de la création, de la maintenance et de la gestion des informations d'identification de l'utilisateur.
Fournisseur de services en ligne	Entité fournissant des services en ligne (applications ou ressources pédagogiques par exemple) à l'utilisateur.
Identification	L'identification consiste à associer une personne physique, un composant ou un élément logiciel à une identité numérique. Les principaux modes d'identification sont : • identifiant (adresse email, login, etc.) ; • certificat.
Infrastructure de gestion de clés publiques	Ensemble de personnel, politique, procédures, composants et facilités qui lient l'identité de l'individu à deux clés cryptographiques asymétriques. La clé privée doit être protégée ; elle permet de signer les données (documents électroniques, message d'authentification) ou de déchiffrer des informations (message, fichier, …), qui ont été au préalable chiffrées avec la clé publique associée. La clé publique est transmise aux entités avec lesquelles l'individu est amené à échanger des informations ; elle permet de vérifier la signature engagée avec la clé privée correspondante ou de chiffrer des informations.
One Time Password ou mot de passe à usage unique	Ce procédé repose sur des techniques de clés symétriques. Le mot de passe est calculé par concaténation d'un secret connu par l'utilisateur et d'un secret généré dynamiquement par une « calculette ». Le mot de passe n'est vérifiable que par le serveur d'authentification et ne peut être rejoué.
Profil	Ensemble d'attributs liés à un utilisateur dont le service d'autorisation déduit les droits.
Référence opaque	Message court codé permettant d'identifier un utilisateur, un groupe ou une communauté de confiance rattachés à un ENT. Ce code est partagé entre les services dans le cadre d'échange entre ENT ou entre un ENT et un fournisseur de service tiers. Cette référence peut être temporaire (valide le temps d'une session) ou permanente (dans le cas de la fédération d'identité).
Reverse Proxy SSO	Voir « Cadres de référence fonctionnel et technique »
Serveur/Agent SSO	Voir « Cadres de référence fonctionnel et technique »
Service en ligne	Ensemble de ressources ou d'applications mises à disposition des usagers sous un format électronique. L'accès à un service en ligne s'effectue par l'intermédiaire d'un client réseau.

3. L'implémentation des services AAS dans l'ENT

3.1. Panorama de la problématique AAS

Ce paragraphe présente l'articulation entre les entités impliquées dans l'ENT et les positionne dans le contexte global de mise à disposition de services numériques aux élèves, étudiants, enseignants et personnels administratifs.

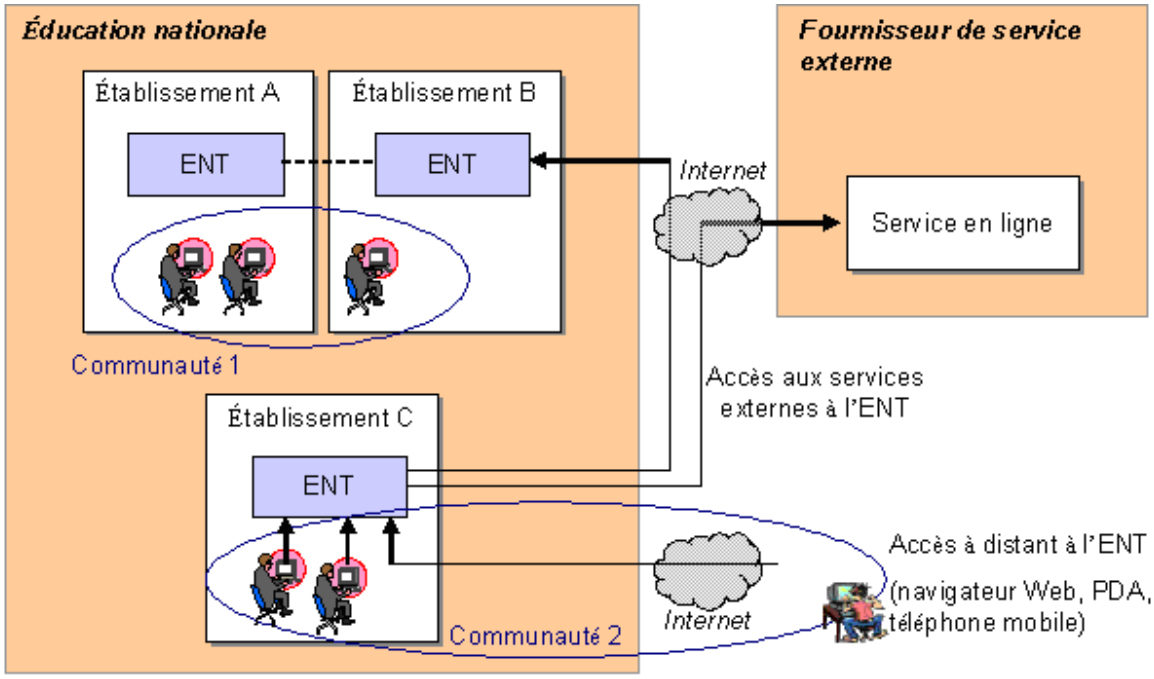

Figure 2 : exemple de représentation des relations entre les entités impliquées dans un ENT

Les entités impliquées sont :

- les établissements à travers l'ENT ;
- les fournisseurs de services externes comme les partenaires publics, les entreprises, les éditeurs, etc.
- les utilisateurs des services équipés d'un client (navigateur Web, PDA, téléphone mobile).

Un ENT est rattaché à une communauté de confiance qui fournit une identité unique à chaque utilisateur qui s'y inscrit. Les utilisateurs dépendent physiquement d'un établissement ; par contre, une communauté PEUT couvrir une population d'utilisateurs répartie sur plusieurs établissements (notamment dans le cadre du scolaire) ou une partie de l'établissement.

Tout utilisateur souhaitant accéder à son ENT et à ses services DOIT être identifié et authentifié de manière unique. L'ensemble des services de sécurité liés au contrôle d'accès et à la gestion des identités et des autorisations fait partie du socle de l'ENT et est décrit au paragraphe 3.2.
Ce document adresse les recommandations AAS aux applications et ressources des ENT.

Les applications traditionnelles (transactionnelles, client / serveur, etc.) n'entrent pas dans le cadre de ces recommandations. Dans le cas d'applications Web antérieures à ces recommandations, il conviendra d'essayer de tendre vers la cible préconisée par ce document.

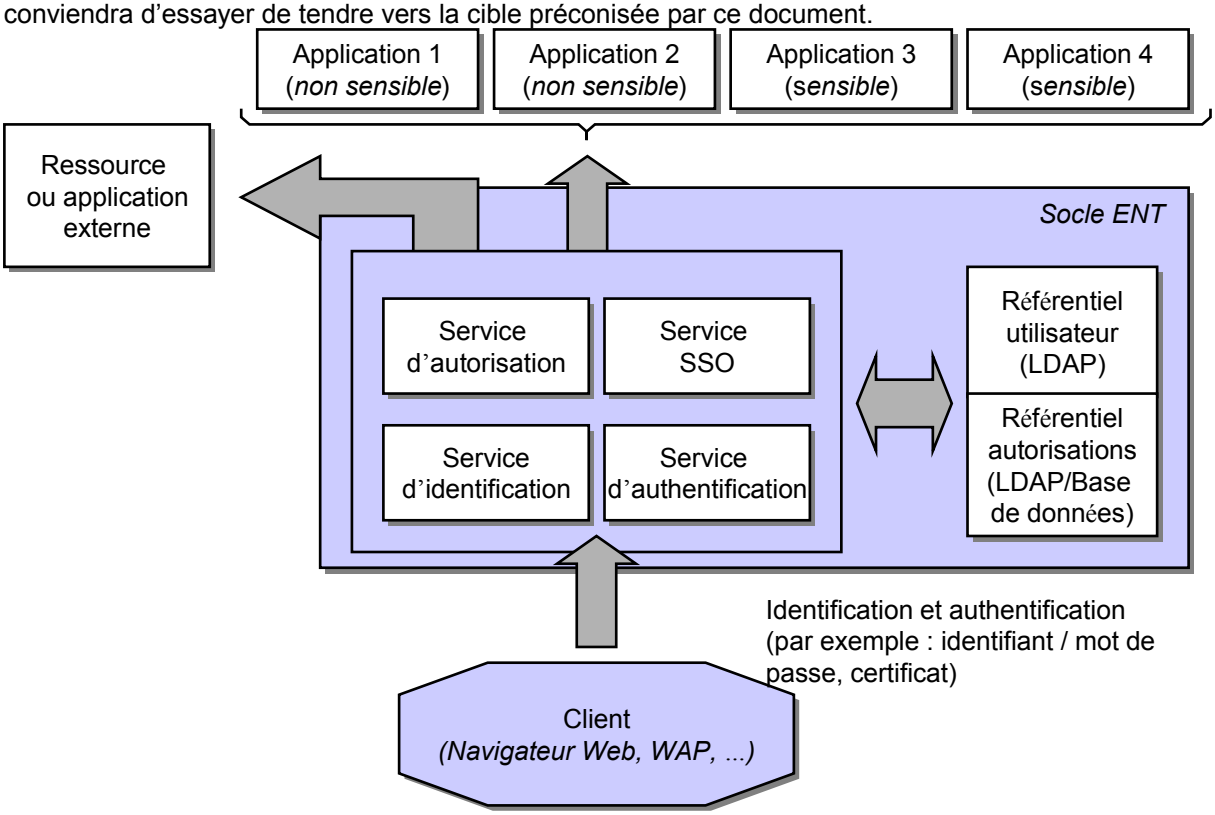

Figure 3 : représentation du socle ENT dans l'architecture globale de l'établissement

3.2. L'architecture générale AAS dans l'ENT

La sécurisation des accès aux espaces numériques de travail et la propagation de l'identité ou du profil des utilisateurs aux différents services numériques reposent sur quatre services :

- service d'identification dont le rôle est de fournir et gérer les identités utilisateurs : enregistrement de l'utilisateur, politique d'identification (règle sur le format de l'identifiant notamment), maintenance des identités (vérification des doublons, …),
  -
- service d'authentification dont le rôle est essentiellement de vérifier l'identité de l'utilisateur auprès du référentiel utilisateur ;
- service d'autorisation dont le rôle est de gérer et d'appliquer les autorisations rattachées à une identité ou à un profil ;
- service de SSO dont le rôle principal est de propager les identités.

Ces quatre services font partie du socle des espaces numériques de travail (*socle ENT) :*

Les composants de l'infrastructure intervenant dans le cadre de projet AAS sont :

- le socle ENT ;
- les services d'annuaires (référentiels utilisateur et référentiels d'identité numérique) ;
- les services applicatifs (portail Web, applications, etc.) ;
- les services de sécurité périphériques (IGC par exemple) ;
- le client (navigateur Web, interface WAP, PDA, …).

4. L'identification et l'authentification des utilisateurs

4.1. Format de l'identifiant

L'utilisateur qui se connecte à l'ENT DOIT disposer d'un identifiant lui permettant d'être identifié et authentifié auprès des services de l'ENT.

Cet identifiant PEUT se représenter selon trois formats :

- un identifiant institutionnel ;
- un alias associé reconnu au sein de sa communauté uniquement ;
- un certificat.

Il DOIT être unique au sein du référentiel d'identité.

Le référentiel utilisateur contient les identifiants et les profils macroscopiques de l'utilisateur. Il repose généralement sur une technologie LDAP.

L'utilisateur DOIT s'identifier auprès de son ENT de rattachement (établissement ou rectorat). Il PEUT utiliser son identifiant institutionnel ou son alias.

4.1.1. Identifiant institutionnel

Le choix des règles de nommage des identifiants est de la responsabilité de l'établissement. Par défaut, le formatage de l'identifiant institutionnel répond aux règles de construction des adresses email. Si elles s'avèrent inadaptées, il convient d'utiliser les « bonnes pratiques » décrites dans ce chapitre.

L'identifiant DEVRAIT être représenté sous la forme canonique suivante : *prenom.nom@nom_domaine*. Il DOIT être non sensible à la casse.

Les homonymies sont réglées par l'insertion d'un numéro séquentiel à la suite du nom en fonction de l'ordre de recensement de ces homonymies. Le numéro est séparé du nom par un tiret. Par exemple :

- pierre.durand pour Pierre Durand, premier enregistré ;
- pierre.durand1 pour le second utilisateur enregistré ;
- pierre.durand2 pour le troisième utilisateur enregistré.

Les prénoms et noms composés sont écrits en entier et raccordés par des tirets et sans accent, par exemple : h*erve.leprince-ringuet* pour Hervé Leprince-Ringuet.

Les blancs sont remplacés par un tiret "-", par exemple : a*ndre.dunoyer-de-segonzac* pour André Dunoyer de Segonzac.

Les apostrophes sont supprimées, par exemple : m*arie-ange-lhelgouarch* pour Marie-Ange l'Helgouarc'h.

Les particules suivent l'ordre normal d'élocution, et non la forme littéraire j*ean-marie.de-lattre-de-tassigny* pour Jean-Marie de Lattre de Tassigny.

Le nom de domaine (valeur *nom_domaine*) correspond à celui de l'établissement ou du rectorat. Par exemple, *univ-rennes1.fr* pour l'université Rennes 1.

Lorsqu'un utilisateur se connecte à son ENT, il PEUT ne saisir que la partie gauche de son identifiant institutionnel (avant @nom_domaine). Le nom de domaine est alors ajouté par le service d'identification de l'ENT.

4.1.2. Alias associé à l'identifiant institutionnel

Pour des raisons de convivialité ou de facilité d'accès, un alias PEUT être associé à l'identifiant institutionnel. L'alias est choisi par l'utilisateur.

L'alias n'est reconnu qu'au sein de l'ENT. Il doit être unique dans l'établissement et cette unicité est gérée selon la règle « premier demandeur, premier servi ».

4.1.3. Certificat associé à l'identifiant institutionnel

Pour renforcer le niveau d'authentification de certaines applications, les établissements PEUVENT fournir aux utilisateurs un certificat électronique. Dans ce cas, le service d'identification associe le certificat, utilisé comme moyen d'authentification forte, à l'identifiant de l'utilisateur.

Le certificat DOIT être :

- émis par une autorité reconnue par les services offerts par les établissements ;
- en cours de validité (non révoqué, non expiré).

4.2. Niveaux d'authentification

Deux niveaux d'authentification sont retenus :

- niveau d'authentification faible : par couple identifiant / mot de passe ;
- niveau d'authentification forte : par certificat ou One Time Password.

Les ENT DOIVENT être accessibles de tout lieu, public ou privé (établissement, domicile, cyber-café, etc.). L'accès à la page d'accueil de l'ENT DOIT pouvoir se faire par une authentification faible car elle ne véhicule pas de données sensibles.

L'ENT donne accès à des services, dont certains sont des applications métiers sensibles (financières par exemple) nécessitant une authentification forte.

Il est de la responsabilité de l'établissement qui déploie l'ENT de déterminer quels services requièrent une authentification forte. Peu de services à authentification forte devraient être accessibles à travers l'ENT, du moins dans les premières phases de leurs déploiements.

Exemples de services à authentification faible : bureau numérique, outils de travail collaboratif, informations en ligne, cours en ligne, consultation de son dossier administratif, etc.

Exemples de services à authentification forte : modification des dossiers administratifs, engagements financiers, etc.

4.3. Confidentialité et intégrité des échanges d'informations d'identités

4.3.1. Entre le client et le socle ENT

Les informations échangées entre le client et le socle ENT pendant les phases d'identification et d'authentification DOIVENT être chiffrées en faisant appel, à minima, aux propriétés du protocole

SSLv3 ou TLS v1.0. Ceci implique que le serveur gérant l'authentification DOIT posséder une certificat électronique. On DOIT s'appuyer sur un certificat dont la qualité sera suffisante pour que l'utilisateur puisse valider l'authenticité de l'ENT.

Typiquement, le mot de passe NE DOIT PAS circuler en clair sur le réseau (entre le client de l'utilisateur et le socle ENT).

Le canal sécurisé établi pendant ces phases PEUT être maintenu pour sécuriser les échanges d'informations dans le cas de traitement de données sensibles.

4.3.2. Entre services

Le mot de passe NE DOIT PAS être transmis aux applications.

On DOIT garantir l'intégrité des échanges d'informations d'identification et d'authentification. On PEUT s'appuyer sur un certificat électronique qui puisse être facilement vérifiable par les entités utilisatrices.

Une relation de confiance DOIT être établie entre les services du socle ENT, les services applicatifs et les ressources. Cette relation de confiance DOIT être établie par une authentification forte par certificats entre les serveurs supportant ces services.

Une fois cette relation de confiance établie, les services PEUVENT s'échanger des attributs d'identification et d'autorisation.

4.4. Intégrité des échanges pendant les phases de contrôle d'accès

Afin de garantir l'intégrité des informations d'identité échangées entre les serveurs de sécurité et applicatifs, les messages (requêtes et réponses) contenant des attributs relatifs à l'identification, l'authentification et l'autorisation d'accès des utilisateurs DEVRAIENT être signés. Ce procédé requiert un certificat électronique.

On entend par serveur, toute machine physique ou logique qui intervient dans le processus de contrôle d'accès. Cinq catégories de serveurs sont référencées dans le cadre de l'ENT :

- identification et authentification ;
- gestion des autorisations ;
- Single Sign-On ;
- référentiel utilisateur ou annuaire LDAP ;
- application ou ressource (Web ou « back office »).

5. La gestion et l'application des autorisations

Il convient de distinguer deux niveaux d'autorisations :

- les autorisations macroscopiques, c'est-à-dire l'accès aux services proposés à l'utilisateur. elles DOIVENT être gérées par le socle ENT (et PEUVENT être stockées dans un annuaire LDAP). Ces informations permettent notamment de construire la page d'accueil de l'ENT en fournissant la liste des services numériques accessibles par l'usager et son profil macroscopique pour chaque service (par exemple élève, étudiant, enseignant, administratif, etc.) ;
- les autorisations microscopiques, c'est-à-dire l'accès aux fonctionnalités et aux données propres à un service ; elles DEVRAIENT être gérées au niveau de l'application (base de données, annuaire LDAP, fichiers plats)

Un concepteur d'application PEUT demander d'ajouter un attribut dans le référentiel d'autorisations (annuaire LDAP ou base de données) qui permet à l'application ou à une ressource de consulter les informations de droit d'accès de l'utilisateur.

Les informations de l'annuaire des utilisateurs PEUVENT être communiquées aux applications selon deux modes :

- le service d'autorisation du socle ENT transmet les informations à l'application en s'appuyant sur le référentiel de gestion des autorisations ;
- l'application demande ces informations directement auprès du référentiel de gestion des autorisations.

Le socle ENT DEVRAIT permettre de définir le format et la méthode d'échange des messages d'identification et d'autorisation. La formalisation de la gestion des autorisations (standard XACML) est trop récente pour valider les recommandations relatives à ce service.

6. La propagation des identités ou des attributs

Dans ce paragraphe, il convient de distinguer les services (ou applications) de SSO internes à l'ENT et externes à l'ENT.

On appelle services internes à l'ENT les applications directement intégrées sur le socle. On appelle services externes à l'ENT les applications fournies par un ENT d'une autre communauté ou celles d'un fournisseur de service externe.

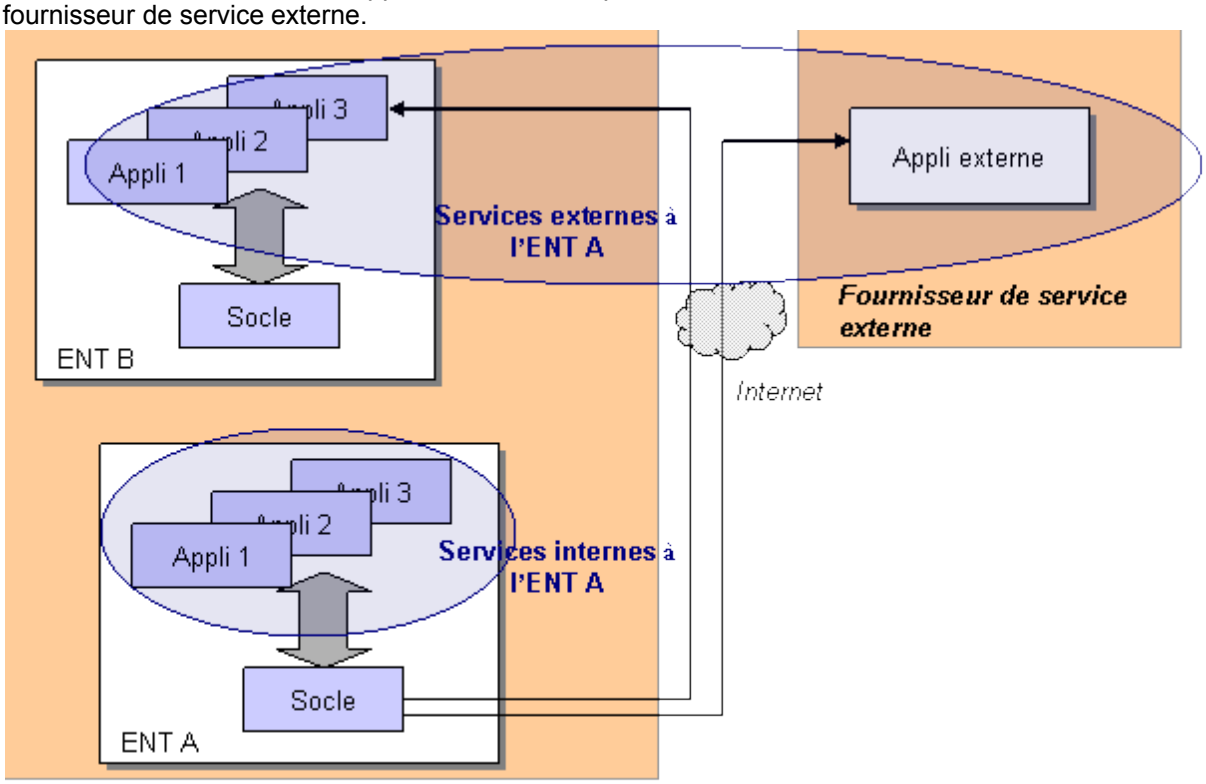

Figure 4 : services internes et externes à l'ENT

6.1. Cas de services internes à l'ENT

Le service de SSO interne à l'établissement PEUT répondre aux propres règles d'implémentation de l'ENT de l'établissement. Étant donné le manque de maturité des standards dans ce domaine, le système de SSO PEUT reposer sur des méthodes de propagation des identités ou des profils spécifiques.

Le mécanisme d'authentification DOIT être assuré par le service SSO et non par l'application.

La propagation des identités est assurée par des outils logiciels SSO qui PEUVENT reposer sur deux types d'architectures : Reverse Proxy ou Serveur/Agent SSO.

Seuls les attributs ou les identités PEUVENT être propagées. Le mot de passe NE DOIT PAS remonter vers les applications.

Le fournisseur d'applications DOIT s'assurer que la librairie d'authentification des applications, utilisées dans l'ENT de l'établissement, est facilement intégrable au service de SSO d'un autre ENT. Autrement dit, le module SSO doit être interchangeable.

6.2. Cas de services externes à l'ENT

Les informations liées à un utilisateur ou à un profil d'utilisateur échangées entre les entités DOIVENT être signées et chiffrées (ou codées) de manière à les rendre illisibles par un tiers.

Les échanges d'informations d'identification et d'autorisation avec des services externes DEVRAIENT reposer sur des échanges de messages SAML. Ces messages sont encapsulés dans des requêtes SOAP sur HTTP.

L'état de l'art ne permet pas d'établir des recommandations précises sur ce format d'échanges et sur les procédures de propagation et de fédération d'identité ou d'attributs.

Les spécifications de la phase 2 de Liberty Alliance, qui seront disponibles en septembre 2003, pourraient fournir un cadre d'interopérabilité pour les services externes si elles répondent aux besoins de l'Éducation nationale(www.projectliberty.org).

L'accès à des services externes à l'ENT de l'utilisateur DEVRAIT reposer sur les notions de partage d'attributs en gardant pour objectif de conserver l'anonymat des utilisateurs.

Pour assurer l'anonymat de l'utilisateur, une référence DOIT être partagée entre les services de sécurité du socle ENT de l'établissement et les services ou ressources internes ou externes à l'ENT de l'utilisateur. Cette référence DOIT être lisible uniquement des services de tout ENT ou tiers adhérant à l'espace de confiance de l'Éducation nationale. Elle DOIT permettre d'associer des attributs ou un identifiant à un utilisateur ou à un profil.

Aucun mot de passe NE DOIT être échangé entre l'ENT de l'utilisateur et les autres ENT ou les fournisseurs de services en ligne tiers.

7. Traçabilité des opérations AAS

Toutes les opérations relatives au contrôle d'accès DOIVENT être tracées à chaque niveau de la chaîne de sécurité de l'ENT.

8. Annexe 1 : constitution du groupe de travail

Le groupe de travail est constitué (par ordre alphabétique) :

- Aubry Pascal, université de Rennes 1
- Baudequin Jean-Michel, Direction de la technologie
- Beaud Christophe, AMUE
- Cadé François, SIIG universités de Strasbourg
- Chung Nicolas, Direction de la technologie
- Dubreuil Christophe,Lycée Général et Technologique Jacques de Vaucanson
- François Sébastien , DICTAO
- Gautier Stéphane, CRDP de l'Académie d'Orléans-Tours
- Jaume Hervé, ULP multimédia
- Le Berre Claude, ULP multimédia
- Le Guigner Jean-Paul, CRU
- Lehoux Jean-Marc, DPMA
- Mathieu Vincent, université de Nancy 2
- Pillou Jean-Francois, Direction de la technologie
- Moisy Jean-Louis, ENS Lyon
- Pantin Jacques, DICTAO
- Saive Claude, DPMA
- Salaun Olivier, CRU
- Vatré Richard, université Paris V