Schéma directeur des espaces numériques de travail

Annexe AAS

Authentification-Autorisation-SSO

Version 2.0

SOMMAIRE

1. Introduction

1.1 Contexte

Le Schéma Directeur des Espaces numériques de Travail (SDET) [1] propose un ensemble de recommandations fonctionnelles, organisationnelles et techniques pour guider la mise en œuvre d'Espaces Numériques de Travail (ENT) dans les établissements d'enseignement.

En complément des grandes orientations proposées dans le document central du SDET, des thèmes sont traités de manière approfondie dans des annexes indépendantes :

- L'annexe « Recommandations pour l'Authentification–Autorisation–SSO : AAS » :

  Elle est consacrée à la sécurisation des accès aux services applicatifs proposés au travers des ENT.

- L'annexe « Juridique » [2] :

  Elle analyse les différentes problématiques juridiques qui peuvent se poser lors de la mise en œuvre et l'exploitation d'un ENT et des conditions de son utilisation.

- L'annexe « Stratégie d'exploitation » [3] :

  Elle apporte des préconisations sur l'organisation de l'exploitation des ENT (maintenance, niveaux de qualité de service, disponibilité…).

- L'annexe « Interopérabilité » [4] :

  Elle définit les standards à suivre et les conditions à respecter pour qu'un ENT soit interopérable avec les autres.

- L'annexe « Recommandations SUPANN » [5] :

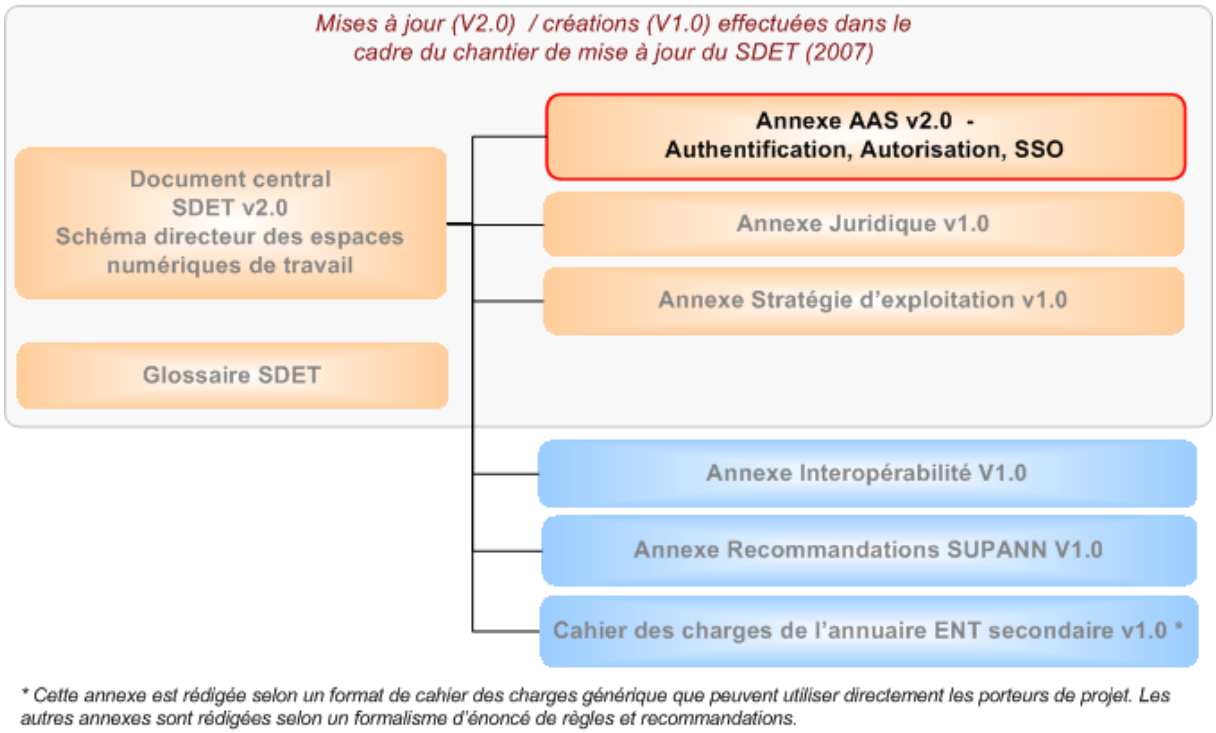
  Elle émet des préconisations pour la compatibilité des annuaires de l'enseignement supérieur.

- L'annexe « Cahier des charges de l'annuaire ENT du secondaire » [6] :

  Elle définit un cahier des charges générique pour la fourniture d'une solution d'annuaire pour le socle des ENT de l'enseignement secondaire.

- L'annexe « Glossaire du SDET » [7] :

  Elle définit le vocabulaire utilisé dans le SDET et ses annexes.



** Cette annexe est rédigée selon un format de cahier des charges générique que peuvent utiliser directement les porteurs de projet. Les autres annexes sont rédigées selon un formalisme d'énoncé de règles et recommandations.*

Le présent document correspond à l'annexe du SDET consacrée aux « Recommandations pour l'Authentification–Autorisation–SSO : AAS ». Cette version 2.0 a été élaborée par un groupe de travail composé d'experts de la communauté de l'enseignement supérieur et de l'enseignement scolaire qui a notamment tiré parti de ses retours d'expérience lors de la mise en place de services AAS dans les ENT.

1.2 Objectifs et contenu du document

L'annexe AAS fournit un ensemble de recommandations pour la mise en œuvre des services AAS des ENT.

Du point de vue de l'utilisateur, l'objectif est d'accéder, de manière simple, à l'ensemble des services applicatifs auxquels il a droit, de façon sécurisée, dans le respect de la vie privée et en n'ayant à s'authentifier qu'une seule fois par session.

Le respect de ces recommandations permet de remplir les objectifs suivants :

- S'assurer que les services applicatifs disponibles depuis l'ENT pourront utiliser les services AAS pour sécuriser, contrôler ces accès.
- Permettre l'interopérabilité entre les services AAS concourant à la sécurisation de l'accès aux services applicatifs.

Ces recommandations permettront de proposer une interface AAS unique pour la communauté éducative, quels que soient les établissements et la solution d'ENT utilisée, tout en garantissant le maintien des niveaux de fonctionnement et de sécurité attendus.

Les recommandations s'adressent donc aux acteurs suivants :

- Les porteurs de projets ENT.

- Les éditeurs de solutions ENT : ce document doit leur permettre de proposer des solutions conformes aux recommandations sur les services AAS.

- Les organismes partenaires (collectivités locales, académies, ministères) : ce document doit permettre de définir les échanges AAS entre leurs systèmes d'information et les ENT.

- Les prestataires privés : fournisseurs d'applications, éditeurs de services en ligne et de contenus.

Remarque : les référentiels nécessaires à la mise en place des services AAS ne sont pas abordés dans ce document.

1.3 Guide de lecture

Niveaux de recommandation

Afin de déterminer le niveau d'obligation de respect des recommandations fournies dans ce document, la terminologie définie dans le RFC 2119 de l'IETF est utilisée, 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

La définition de ces termes issus du RFC 2119 et appliqués à ce document est la suivante :

- **DOIT** : ce mot, ou le terme « EXIGÉ », signifie que la définition est une exigence absolue de la spécification (i.e. du présent document).

- **NE DOIT PAS** : cette expression signifie que la définition est une interdiction absolue de la spécification (i.e. du présent document).

- **DEVRAIT** : ce mot, ou l'adjectif « RECOMMANDÉ », signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ne pas appliquer cette recommandation, mais les conséquences doivent être comprises et analysées soigneusement avant de choisir une autre option. Remarque : cette recommandation correspond à un conseil ou à une bonne pratique.

- **NE DEVRAIT PAS** : cette expression, ou l'expression « NON RECOMMANDÉ », signifient qu'il peut exister des raisons valables, dans des circonstances particulières, quand le

comportement particulier est acceptable ou même utile, de suivre cette recommandation. Mais les conséquences doivent être comprises et le cas soigneusement pesé.

- **PEUT** : ce mot, ou l'adjectif « FACULTATIF », signifie qu'un item est vraiment facultatif. Un fournisseur 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 fournisseur peut omettre le même item.

Nature des recommandations

Notons que les recommandations du document couvrent deux aspects :

- Certaines recommandations définissent des règles ou des principes à respecter.
- D'autres recommandations indiquent des travaux complémentaires à mener sur lesquels chaque acteur de projets ENT doit se positionner.

Enfin, afin d'étayer le propos, certaines recommandations sont illustrées par des cas d'usage, des retours d'expérience ou des précisions techniques.

1.4 Documents de référence et terminologie

Les documents de référence pour l'application des recommandations sont précisés à la fin de ce document (Documents de référence).

La terminologie utilisée dans ce document est définie dans l'annexe du SDET « Glossaire du SDET » [7].

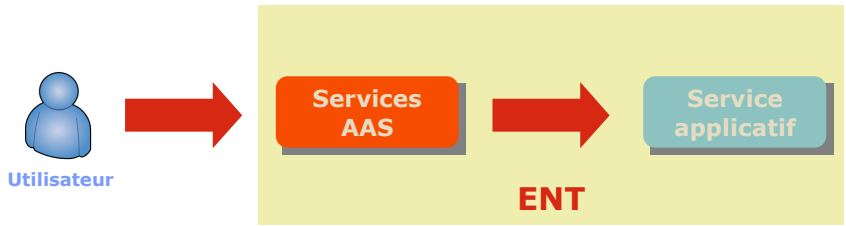
2. Présentation des services AAS des ENT

2.1 Définition des services AAS

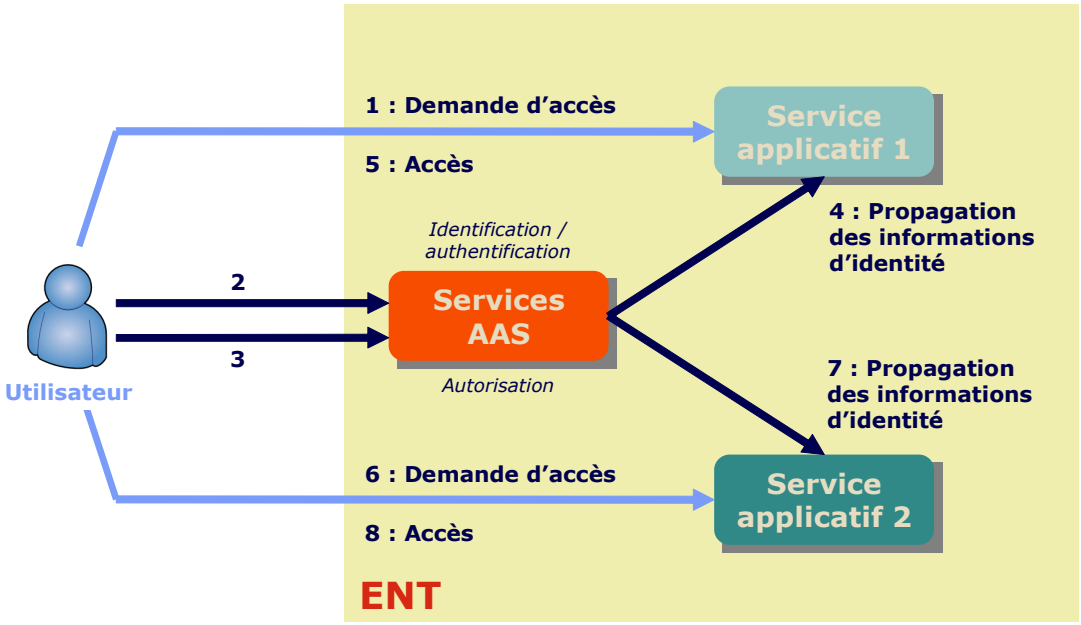
Principes de fonctionnement

Tout utilisateur souhaitant accéder aux services applicatifs disponibles à travers un ENT DOIT être identifié, authentifié et autorisé.

L'accès à ces services applicatifs DOIT être contrôlé par les services AAS. Ils permettent de gérer et de contrôler l'identité et les droits d'accès d'un utilisateur à un service applicatif.



Le principe de fonctionnement des services AAS, sans préjuger des orientations techniques qui peuvent être prises, peut être illustré par la cinématique du schéma suivant :



La cinématique d'accès est la suivante :

1. Un utilisateur non authentifié souhaite accéder à un service applicatif ou à des fonctionnalités ou données propres à un service applicatif.

2. Cette demande d'accès sur une ressource protégée déclenche l'identification et l'authentification de l'utilisateur auprès des services AAS.

3. Une fois l'utilisateur identifié et authentifié, les services AAS autorisent ou non l'accès de l'utilisateur à la ressource.

4. Les services AAS propagent auprès du service applicatif les informations d'identité permettant l'accès de l'utilisateur authentifié, et permettant éventuellement de réaliser un contrôle complémentaire pour autoriser l'accès de l'utilisateur.

5. L'utilisateur accède au service applicatif.

6. L'utilisateur souhaite ensuite accéder dans la même session à un autre service applicatif.

7. Il n'est pas nécessaire qu'il s'identifie et s'authentifie de nouveau auprès des services AAS. Des informations d'identité sont transmises au service applicatif de manière transparente pour l'utilisateur.

8. L'utilisateur accède au service applicatif.

Services AAS

Service d'identification/authentification

Le service d'identification/authentification assure l'authentification des utilisateurs à partir de la réception et de la vérification d'un couple « identifiant / authentifiant ».

Le service d'identification/authentification permet également la gestion du cycle de vie des identités et des authentifiants.

Dans la terminologie SDET, ce service correspond à l'« Authentification » des services « Authentification–Autorisation–SSO ».

Service d'autorisation

Les autorisations définissent quels utilisateurs (caractérisés par un identifiant et un ou plusieurs attributs) peuvent effectuer des actions sur des ressources, éventuellement sous certaines conditions.

Une action sur une ressource définit une habilitation.

Une action peut être une opération de lecture, écriture, modification ou suppression.

Une ressource peut être un service applicatif, une partie de service, une application, une page Web…

Une condition peut être une restriction d'accès au service applicatif, par exemple en fonction de l'horaire ou de la typologie d'accès.

Le service d'autorisation permet de contrôler les autorisations, c'est-à-dire à la fois de vérifier l'existence d'une association entre un utilisateur et une habilitation mais également que les conditions éventuelles sont satisfaites.

Le service d'autorisation permet également la gestion du cycle de vie des autorisations.

Dans la terminologie SDET, ce service correspond à l'« Autorisation » des services « Authentification–Autorisation–SSO ».

Service de propagation des informations d'identité

Ce service permet de propager des informations d'identité dans l'objectif de contrôler l'accès à une ressource.

Les informations d'identité d'un utilisateur peuvent être ses identifiants, ses attributs ou encore les preuves de ses authentifications.

Une preuve d'authentification se définit comme les éléments qui prouvent que l'identité d'un utilisateur a été reconnue via un service d'identification/authentification.

Il existe plusieurs types de preuves d'authentification. Par exemple :

- Preuves signées par un serveur d'authentification : assertions SAML, certificat X.509...
- Preuves validables par un tiers : ticket Kerberos, ticket CAS...

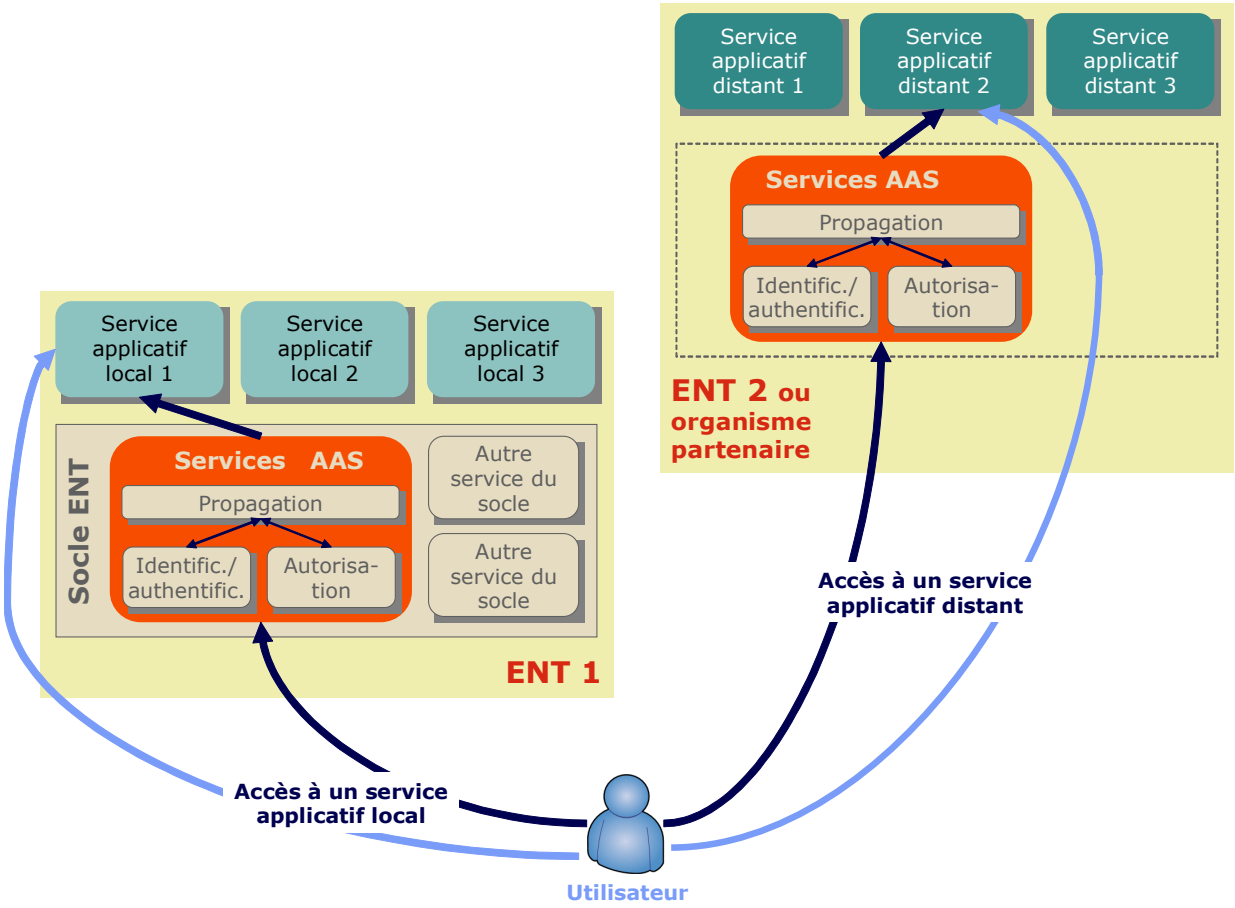
En outre, la propagation de preuves d'authentification peut éviter à l'utilisateur de s'authentifier de nouveau pour accéder à différents services applicatifs, offrant ainsi une fonction de Single Sign-On (SSO).

Dans la terminologie SDET, ce service correspond au « SSO » des services « Authentification–Autorisation–SSO ».

2.2 Architecture générale AAS dans l'ENT

Les services AAS s'intègrent dans le socle d'un ENT, au même titre que les services portail ou les services mutualisés.

Le schéma suivant représente les différentes entités en relation avec un ENT, qui pourront être un autre ENT ou un organisme partenaire (exemples : collectivité, académie, ministère…).



Les services AAS permettent à un utilisateur d'accéder à la fois aux services applicatifs locaux (i.e. proposés par son ENT) mais également à des services applicatifs distants, proposés par les différentes entités en relation avec un ENT.

Remarque : les services applicatifs non Web (transactionnels, client/serveur…) ne rentrent pas dans le cadre des recommandations du présent document. Dans le cas de services applicatifs Web antérieurs à ces recommandations, et qui ne sauraient pas s'appuyer sur les services AAS, il conviendra de tendre vers la cible préconisée par ce document.

3. Identification et authentification des utilisateurs

3.1 Principes pour l'identifiant

Tout utilisateur de l'ENT DOIT posséder au moins un identifiant qui lui permettra d'être identifié et authentifié lors de ses accès aux services applicatifs.

L'unicité de l'identifiant DOIT être garantie à tout moment sur le périmètre d'un ENT donné.

L'identifiant DEVRAIT être invariant.

Remarque : l'invariance de l'identifiant dans le temps (par exemple même si le nom de l'utilisateur change) permet de faciliter la gestion des identifiants.

L'identifiant d'un utilisateur NE DEVRAIT PAS être réaffecté à une autre personne, même si celui-ci n'a plus accès à l'ENT.

Remarque : la non réaffectation de l'identifiant permet de faciliter la traçabilité et l'imputabilité des actions. En tout état de cause, il est nécessaire de se conformer aux recommandations sur la traçabilité telles que définies au chapitre 7.

L'authentification des utilisateurs PEUT être réalisée à partir de l'identifiant ou d'un alias de connexion.

Ainsi, pour des raisons de facilité d'accès, un alias de connexion PEUT être associé à l'identifiant. Cet alias est choisi par l'utilisateur. Il est reconnu au sein d'un ENT donné et il DOIT être unique sur ce périmètre.

Exemple de règle de gestion de l'alias de connexion : un alias donné est attribué à la première personne qui en fait la demande. Il reste valable tant que l'utilisateur le souhaite.

3.2 Moyens d'authentification

3.2.1 Généralités

L'authentification d'un utilisateur DOIT reposer sur la vérification d'un authentifiant. Cet authentifiant est généralement connu ou possédé uniquement par la personne en ayant l'usage.

Le service d'identification/authentification DOIT proposer une authentification par mot de passe.

Le service d'identification/authentification PEUT proposer d'autres moyens d'authentification tels que les certificats et les mots de passe à usage unique ; éventuellement pour un ensemble limité d'utilisateurs.

Le service d'identification/authentification DOIT être le seul service de l'ENT auquel les mots de passe sont directement transmis (à l'exception du service de changement de mot de passe). Les services applicatifs ne reçoivent que les informations d'identités, tel que défini au chapitre 5.

Le même mode de fonctionnement DEVRAIT être mis en place pour les autres moyens d'authentification. Des exceptions sont possibles dans le cas où des services applicatifs exigent des moyens d'authentification non implémentés au niveau du socle ENT.

En particulier, les composants logiciels suivants NE DOIVENT PAS réaliser l'authentification des utilisateurs : les mandataires, les routeurs logiciels, les portails actifs.

Lors de l'accès à un service applicatif, et après identification et authentification de l'utilisateur auprès des services AAS, une session est ouverte. L'ENT DOIT mettre en place une fonction de déconnexion permettant à l'utilisateur de mettre fin à la session.

Suite à une période d'inactivité ou après une certaine durée, les services AAS DOIVENT demander une nouvelle authentification de l'utilisateur pour le maintien de la session.

3.2.2 Mots de passe

Les mots de passe NE DOIVENT PAS être stockés en clair. Les mots de passe DEVRAIENT être stockés de manière chiffrée et irréversible, éventuellement sous forme d'empreintes numériques.

Lors de la vérification du couple « identifiant / mot de passe », le chiffrement et la comparaison avec la valeur stockée du mot de passe DOIVENT être effectués par le service AAS.

Une politique de mot de passe adaptée aux utilisateurs DOIT être définie pour un ENT. Elle PEUT différer selon le type d'utilisateurs.

Par exemple, elle PEUT reposer sur les critères suivants :

- Dureté ou non trivialité : longueur minimale, règles de syntaxe, combinaison imposée de caractères spéciaux, dictionnaires…
- Fréquence de renouvellement.
- Interdiction de réutiliser des mots de passe précédents ou trop proches des derniers.
- Interdiction d'utiliser un mot de passe contenant des attributs de l'utilisateur.

Le nombre d'échecs successifs de saisie du mot de passe DEVRAIT être tracé.

3.2.3 Mots de passe à usage unique

Un mot de passe à usage unique est un secret généré par un dispositif matériel ou logiciel en possession de l'utilisateur.

Ce mot de passe NE PEUT être utilisé qu'une seule fois pour authentifier l'utilisateur lors de son accès aux services applicatifs de l'ENT.

La gestion des supports délivrant les mots de passe dynamiques DOIT faire l'objet de procédures adaptées telles que définies au chapitre 3.4.

3.2.4 Certificats utilisateurs

Les certificats utilisateurs DOIVENT être émis par une autorité de certification reconnue à la fois par les services d'identification/authentification et par les services applicatifs de l'ENT.

Les certificats utilisables pour identifier et authentifier les utilisateurs DOIVENT être en cours de validité (non révoqués, non expirés).

La gestion des certificats DOIT faire l'objet d'une politique de certification.

La gestion des certificats DOIT faire l'objet de procédures adaptées telles que définies au chapitre 3.4.

3.3 Niveaux d'authentification

En fonction de leur sensibilité (criticité des données, ouverture du service sur réseau public…), les accès aux services applicatifs peuvent nécessiter des niveaux d'authentification différents, apportant plus ou moins de garanties sur l'identité d'un utilisateur.

Les niveaux d'authentification peuvent être liés :

- À la nature des authentifiants à présenter par l'utilisateur pour être authentifié.
- Aux processus de gestion de ces authentifiants.

Chaque ENT DOIT définir :

- Les différents moyens d'authentification pris en charge (cf. chapitre 3.2).
- La hiérarchie de niveau entre ces moyens d'authentification.
- Le moyen d'authentification associé à chaque ressource de l'ENT.

Ainsi, un utilisateur NE DOIT accéder à un service applicatif que s'il est authentifié par un moyen d'authentification dont le niveau est supérieur ou égal au niveau du moyen d'authentification requis par ce service.

Dans le cas contraire, le service applicatif DEVRAIT émettre une demande de nouvelle authentification de l'utilisateur avec un moyen d'authentification de niveau supérieur.

La hiérarchie définie est partagée par tous les services d'un même ENT.

3.4 Gestion du cycle de vie des identités et des moyens d'authentification

Chaque ENT DOIT mettre en place des processus de gestion du cycle de vie des identités et des moyens d'authentification. Les responsabilités sur ces processus DOIVENT être définies.

A minima, les processus suivants DEVRAIENT être définis pour la gestion du cycle de vie des identités :

- Inscription / activation (implicite ou explicite) d'un utilisateur.
- Attribution / retrait d'un identifiant conforme aux recommandations précédemment mentionnées.
- Modification des caractéristiques d'un utilisateur.
- Désactivation / suspension / suppression d'un utilisateur.

A minima, les processus suivants DEVRAIENT être définis pour la gestion du cycle de vie des moyens d'authentification :

- Distribution, mise à jour, renouvellement, retrait des moyens d'authentification et/ou de leurs supports, changement / réinitialisation des mots de passe.
- Révocation, perte, vol, dysfonctionnement des moyens d'authentification.

Remarque : la mise en place du service d'identification/authentification peut nécessiter la mise en place d'un ou plusieurs référentiels de données.

4. Autorisations des utilisateurs

4.1 Contrôle des autorisations

Le contrôle des autorisations pour l'accès aux services applicatifs DOIT être réalisé par le service d'autorisation.

Par exemple, ce service PEUT permettre de construire la page d'accueil de l'ENT en fournissant la liste des services applicatifs accessibles par l'utilisateur.

Le contrôle des autorisations sur des fonctions ou des données propres à un service applicatif PEUT être réalisé par le service d'autorisation ou directement par le service applicatif.

Dans ce dernier cas, et à des fins de contrôle des autorisations, le service applicatif DOIT pouvoir récupérer des informations d'identités (identifiant et attributs) ou des informations sur les habilitations des utilisateurs. Le format et la méthode d'accès à ces informations DOIVENT être définis pour chaque ENT. Le service applicatif PEUT également s'appuyer sur le service de propagation des informations d'identité pour récupérer ces informations.

Enfin, pour réaliser le contrôle des autorisations au niveau du service applicatif, le concepteur dudit service PEUT demander à compléter la caractérisation des utilisateurs ; l'acceptation relève de la responsabilité de chaque ENT.

4.2 Gestion du cycle de vie des autorisations

Chaque ENT DOIT mettre en place des processus de gestion du cycle de vie des autorisations. Les responsabilités sur ces processus DOIVENT être définies.

A minima, les processus suivants DEVRAIENT être définis pour la gestion du cycle de vie des autorisations :

- Attribution / suspension / suppression / modification des autorisations.
- Modification des caractéristiques nécessaires aux contrôles des autorisations.
- Délégation des autorisations (définir quelles autorisations peuvent être déléguées, qui peut déléguer ses autorisations, vers qui, pour combien de temps…).

Remarque : la mise en place du service d'autorisation peut nécessiter la mise en place d'un ou plusieurs référentiels de données.

5. Propagation des informations d'identité

5.1 Propagation des informations d'identité au sein de l'ENT

5.1.1 Généralités

Les services d'identification/authentification et d'autorisation s'appuient sur le service de propagation des informations d'identité pour échanger des informations d'identité avec les services applicatifs locaux.

Ainsi, le service de propagation des informations d'identité DOIT réaliser :

- la transmission des identifiants, des preuves d'authentification (précisant a minima le moyen d'authentification) et d'attributs caractérisant les utilisateurs ;

- la transmission d'informations sur le fait que l'utilisateur est déconnecté de ses sessions aux services applicatifs.

Remarques :

- Seules les informations d'identité (identifiant, preuve d'authentification et attributs) PEUVENT être propagées. Les authentifiants NE DOIVENT PAS être propagés.

- Éventuellement, des informations d'autorisation PEUVENT être transmises. Le contrôle des autorisations PEUT s'appuyer sur ces informations ou bien être réalisé sur la base d'informations complémentaires stockées localement.

5.1.2 Single Sign-On

L'ENT DOIT offrir une fonction de SSO. Cette fonction permet à un utilisateur d'accéder à différents services applicatifs en ne devant s'authentifier qu'une seule fois (tant que l'authentification préalable auprès des services AAS est valable).

Aucune méthode de propagation des preuves d'authentification aux services applicatifs de l'ENT n'est imposée. En revanche, les fournisseurs DOIVENT s'assurer que leurs services applicatifs sont compatibles et intégrables avec la fonction de SSO proposée.

Le service de propagation des informations d'identité DOIT mettre en place des mécanismes permettant la propagation de la déconnexion auprès de l'ensemble des services applicatifs avec lesquels l'utilisateur a une session en cours.

La déconnexion DEVRAIT se traduire par la destruction des preuves d'authentification émises.

5.2 Propagation des informations d'identité hors de l'ENT

5.2.1 Généralités

Le service de propagation des informations d'identité hors de l'ENT a des caractéristiques similaires à celles proposées pour la propagation des informations d'identité au sein d'un ENT.

Une fédération concerne un ensemble d'acteurs de la sphère éducative (ministères, académies, collectivités locales ou autres organismes partenaires), qui coopèrent au sein d'un espace de confiance pour notamment gérer des identités, gérer les autorisations des utilisateurs et contrôler leurs accès.

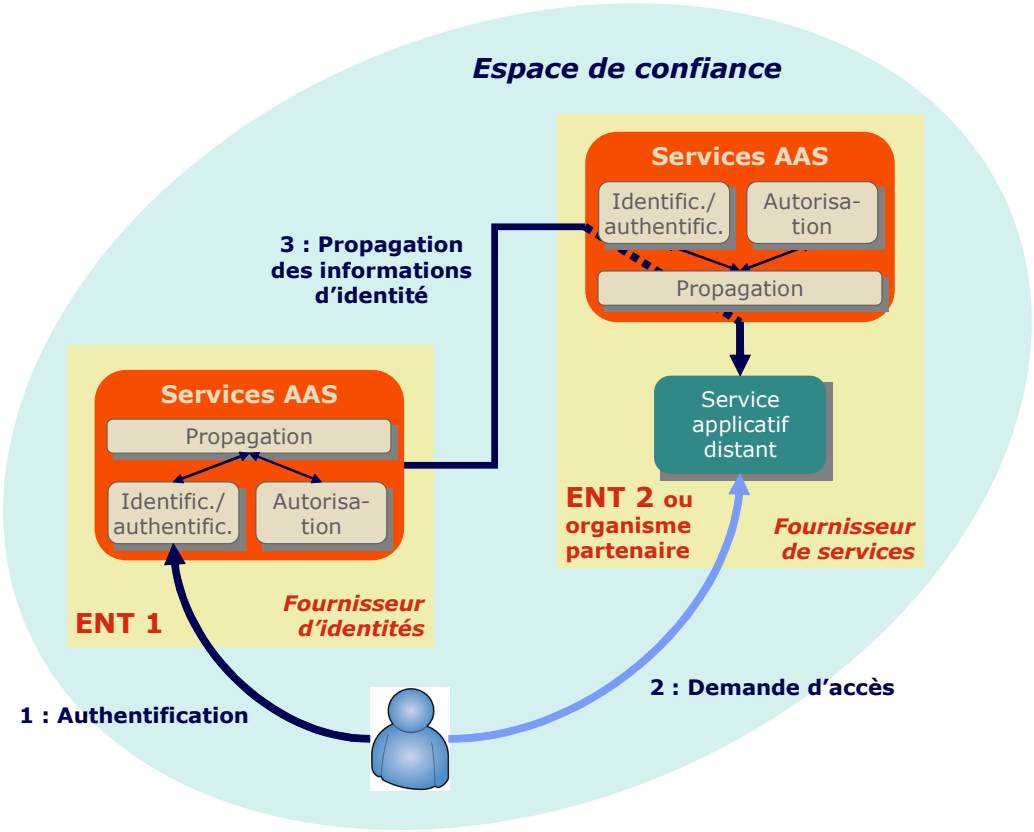
Deux cas d'usages d'un ENT peuvent se présenter :

- Un utilisateur authentifié sur un ENT souhaite accéder à un service applicatif distant. Cela nécessite de transmettre des informations d'identité depuis l'ENT vers le fournisseur de services. L'ENT joue ici le rôle de fournisseur d'identités, et éventuellement de fournisseur d'attributs.

- Un utilisateur authentifié auprès d'un fournisseur d'identités souhaite accéder à un service applicatif proposé par l'ENT. L'ENT reçoit de ce fournisseur d'identités des informations

d'identité. Sur cette base, le contrôle d'accès au service applicatif peut alors s'effectuer. L'ENT joue ici le rôle de fournisseur de services.

Ces deux cas d'usage sont présentés simultanément sur la figure ci-dessous. En effet, les deux acteurs peuvent être des ENT, ce qui signifie que l'ENT 1 représente le fournisseur d'identités, alors que l'ENT 2 représente le fournisseur de services.



L'espace de confiance de la fédération DOIT être régi par un cadre général de règles. Ces règles DOIVENT notamment déterminer les engagements des fournisseurs d'identités et des fournisseurs de services.

Chaque membre de la fédération DOIT pouvoir définir, en complément du cadre général, les relations unitaires qu'il souhaite établir avec chacun des autres membres. En particulier, un fournisseur d'identités DOIT pouvoir décider quels sont les attributs qu'il accepte de transmettre à chacun des fournisseurs de services.

5.2.2 Données partagées

Afin d'assurer le fonctionnement de la fédération, et notamment de réaliser le contrôle des accès des utilisateurs aux services applicatifs, il est nécessaire de définir des données communes à tous les membres de la fédération. En particulier :

- Les attributs caractérisant les utilisateurs et nécessaires au contrôle des accès DOIVENT suivre un nommage et une sémantique communs au sein de la fédération.

  Par exemple, l'annexe « Recommandations SUPANN » [5] définit des attributs qui pourraient être, pour tout ou partie, communs à une fédération.

- Les moyens d'authentification partagés DOIVENT être définis de manière commune dans toute la fédération.

5.2.3 Fonctions proposées

Lorsqu'un ENT assure le rôle de **fournisseur d'identités**, les fonctions du service de propagation des informations d'identité hors de l'ENT sont les suivantes :

- Le service DOIT permettre l'anonymisation des identités : l'identifiant ou l'alias de connexion n'est pas transmis, ou bien un autre identifiant non significatif (i.e. opaque) et non persistant est transmis.

- Le service DEVRAIT permettre la pseudonymisation des identités : l'identifiant ou l'alias de connexion n'est pas transmis. À la place, un identifiant non significatif (i.e. opaque) mais persistant (pour un service donné) est transmis. Ce pseudonyme PEUT être différent en fonction de chaque service applicatif distant accédé.

- Le service DEVRAIT permettre aux utilisateurs de limiter individuellement et au cas par cas les attributs transmis aux fournisseurs de services.

  Remarque : les règles de la CNIL ne rendent pas indispensables le contrôle des attributs propagés par l'utilisateur, en cas d'usages légitimes (autorisation d'accès).

- Afin de garantir la traçabilité, le fournisseur d'identités DOIT être capable à tout instant de faire le lien entre les informations d'identité transmises et l'identifiant de l'utilisateur.

Lorsqu'un ENT assure le rôle de **fournisseur de services**, les fonctions du service de propagation des informations d'identité hors de l'ENT sont les suivantes :

- Le service de propagation des informations d'identité hors de l'ENT DOIT permettre au service applicatif demandé d'interpréter une preuve d'authentification venant d'un service d'identification/authentification extérieur.

Quel que soit le rôle de l'ENT, les fonctions complémentaires du service de propagation des informations d'identité hors de l'ENT sont les suivantes :

- Le service DOIT assurer la conversion entre les preuves d'authentification utilisées au sein de l'ENT et les preuves d'authentification partagées au niveau de la fédération.

- Le service DOIT assurer la conversion entre les moyens d'authentification définis au sein de l'ENT et les moyens d'authentification partagés au niveau de la fédération.

- Le service DOIT assurer la conversion entre les attributs utilisés au sein de l'ENT et ceux utilisés dans le cadre de la fédération (nommage et sémantique).

5.2.4 Règles de la fédération

Les engagements suivants PEUVENT être définis pour les **fournisseurs d'identités** :

- Respect de l'objet et des règles communes de fonctionnement de la fédération.

- Gestion des identités, des moyens d'authentification et des autorisations selon des procédures formalisées et diffusées.

- Action en conformité avec les règles relatives aux données nominatives type CNIL.

- Respect de règles de sécurité.
- Définition, mise à jour et respect des données partagées.
- Définition le cas échéant d'une notion d'identifiant unique sur le périmètre de la fédération et de sa forme.
- Utilisation des standards technologiques définis.
- Journalisation des usages du service d'identification/authentification.

Les engagements suivants doivent être pris par les **fournisseurs de services** :

- Respect de l'objet et des règles communes de fonctionnement de la fédération.
- Gestion des identités et des autorisations selon des procédures formalisées et diffusées.
- Action en conformité avec les règles relatives aux données nominatives type CNIL.
- Respect de règles de sécurité.
- Utilisation des standards technologiques définis.

5.2.5 Gestion du cycle de vie des règles de la fédération

La coordination de la fédération DOIT être assurée, notamment afin de :

- Définir l'organisation de la fédération.
- Définir et faire vivre l'objet et les règles communes de fonctionnement de la fédération.

La fédération DOIT être administrée, notamment afin de :

- Définir le statut administratif.
- Définir et distribuer les données partagées par tous les membres.
- Définir les orientations technologiques supportées (standards utilisés) et les règles de sécurité à suivre.
- Traiter les demandes d'inscription et de départ.
- Contrôler les engagements des membres de la fédération.
- Appliquer les évolutions des règles de fonctionnement.

5.2.6 Recommandation technologique

Les mécanismes de propagation des informations d'identité (identifiants, preuves d'authentification et attributs) hors de l'ENT DOIVENT reposer sur la norme SAML 2.0 (*Security Assertion Markup Language*).

Remarque : Les recommandations fonctionnelles et technologiques concernant la propagation des informations d'identité hors de l'ENT devront également s'appliquer aux Web Services.

6. Confidentialité et intégrité des échanges

6.1 Phase d'identification/authentification

Les échanges pendant les phases d'identification et d'authentification s'effectuent entre l'utilisateur et le service d'identification/authentification du socle ENT.

La confidentialité et l'intégrité des informations d'identification et d'authentification échangées DOIVENT être assurées de bout en bout.

Par exemple, les mots de passe NE DOIVENT PAS être déchiffrés puis chiffrés de nouveau successivement par des éléments intermédiaires.

Le chiffrement permet d'assurer la confidentialité des échanges, par exemple en faisant appel aux protocoles SSLv3 ou TLSv1.

De même, il est possible de s'appuyer sur un certificat pour assurer l'intégrité des échanges d'informations d'identification et d'authentification, certificat qui doit être facilement vérifiable par les entités utilisatrices.

6.2 Phase de propagation des informations d'identité

Les échanges d'informations d'identité s'effectuent entre les services de propagation des informations d'identité, ou entre les services de propagation et les services applicatifs locaux ou distants.

Remarque : le client réseau de l'utilisateur, et éventuellement d'autres composants de la chaîne de liaison applicative, peuvent être impliqués dans les échanges d'informations d'identité en tant que relais.

Lors de ces échanges, l'identité des services impliqués ou des serveurs supportant les services en question DOIT être garantie, par exemple à travers une authentification par certificat.

Cette recommandation est FACULTATIVE pour les échanges au sein d'un ENT.

La confidentialité et l'intégrité des échanges d'informations d'identité DOIVENT être assurées de bout en bout.

Si le client réseau de l'utilisateur est utilisé en temps que relais, un canal sécurisé est établi entre celui-ci et le service applicatif pour garantir la confidentialité et l'intégrité des échanges d'informations d'identité. Ce canal PEUT être maintenu pour sécuriser l'échange d'autres données, par exemple des données applicatives.

7. Traçabilité des opérations AAS

L'ENT DOIT garantir la traçabilité des opérations AAS, permettant de répondre aux besoins suivants :

- Analyse a posteriori en cas d'incident de fonctionnement, d'abus d'utilisation ou d'audit de sécurité.
- Respect des obligations réglementaires[1].

Les journaux produits DOIVENT être exploitables. Ils DOIVENT permettre à tout moment :

- de dater et d'associer une opération AAS à une identité ;
- de reconstituer la chaîne des opérations AAS liées à une identité.

Cette recommandation s'applique également pour les opérations AAS impliquant plusieurs ENT ou organismes partenaires.

Des moyens permettant d'assurer l'intégrité des journaux et le contrôle d'accès à ces journaux DEVRAIENT être mis en place.

Les modalités de ces journalisations DOIVENT respecter la législation en vigueur (données, durée de conservation, moyens de recouvrement…).

8. Documents de référence

N°	Documents de référence MENESR	Source
[1]	SDET	Schéma Directeur des Espaces numériques de Travail. http://www2.educnet.education.fr/sections/services/ent/sdet/
[2]	Annexe « Juridique »	Annexe du SDET sur les problématiques juridiques de mise en œuvre, d'exploitation et d'utilisation d'un ENT. http://www2.educnet.education.fr/sections/services/ent/sdet/
[3]	Annexe « Stratégie d'exploitation »	Annexe du SDET sur l'organisation de l'exploitation des ENT. http://www2.educnet.education.fr/sections/services/ent/sdet/
[4]	Annexe « Interopérabilité »	Annexe du SDET sur la définition des standards à suivre et des conditions à respecter pour qu'un ENT soit interopérable avec les autres. http://www2.educnet.education.fr/sections/services/ent/sdet/

[1] Des précisions sur les obligations règlementaires liées à la traçabilité sont données dans l'annexe « Juridique » [2].

N°	Documents de référence MENESR	Source
[5]	Annexe « Recommandations SUPANN »	Annexe du SDET sur le projet d'annuaires pour les établissements d'enseignement supérieur. http://www2.educnet.education.fr/sections/services/ent/sdet/
[6]	Annexe « Cahier des charges de l'annuaire ENT »	Annexe du SDET définissant un cahier des charges génériques pour les annuaires ENT de l'enseignement secondaire. http://www2.educnet.education.fr/sections/services/ent/sdet/
[7]	Annexe « Glossaire du SDET »	Annexes du SDET définissant le vocabulaire utilisé dans le SDET et ses annexes. http://www2.educnet.education.fr/sections/services/ent/sdet/
[8]	Schéma Directeur de la Sécurité des Systèmes d'Information	Organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives. http://www.orion.education.fr/dpma-a3

Normes et standards	Source
Liberty Alliance	Consortium d'éditeurs définissant des standards pour la fédération des identités. http://www.projectliberty.org
OASIS	Organization for the Advancement of Structured Information Standards : consortium international pour la standardisation des technologies liées aux Web Services. http://www.oasis-open.org
SAML	Simple Authentication Markup Language : standard OASIS définissant un framework XML pour la création, la demande et l'échange de messages d'authentification. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
Shibboleth	Norme de fédération des identités et implémentation logicielle open-source pour le partage des ressources Web avec contrôle d'accès. http://shibboleth.internet2.edu
WS-Federation	Brique de fédération de la suite WS-* (suite de spécifications initiée par Microsoft pour les Web Services). http://specs.xmlsoap.org/ws/2003/07/secext/WS-Federation.pdf
WS-Security	Standard OASIS définissant un ensemble de mécanismes permettant de sécuriser les échanges de messages entre Web Services. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
XACML	eXtensible Access Control Markup Language : standard OASIS pour la définition des échanges de messages de contrôle d'accès. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml