Innovation technologique dans les établissements scolaires : l'ENT, les impacts sur l'organisation du travail et les risques associés

Version destinée aux enseignants qui exercent dans des établissements qui possèdent un ENT

Propriétés	Description
Intitulé court	Les effets de la mise en place d'un Espace Numérique de Travail (ENT) au sein d'un établissement scolaire
Intitulé long	L'impact organisationnel et les risques informatiques suite à la mise en place d'un ENT au sein d'un établissement scolaire
Présentation	Cette ressource est destinée aux enseignants qui exercent dans des **établissements qui possèdent un Espace Numérique de Travail**. À l'aide d'interview, de manipulations et d'une analyse documentaire, l'élève est amené à : • identifier les changements induits sur les modes de travail, de coordination et d'échange entre acteurs dans une organisation, • relier ces changements aux caractéristiques des solutions numériques utilisées, • repérer différents types de risques liés au fonctionnement et à l'usage des technologies numériques, • proposer des solutions de sécurisation en réponse aux risques identifiés et aux obligations d'une organisation concernant la protection des données personnelles.
Formation concernée	Classe de terminale SIG de la série Sciences et Technologie du Management et de la Gestion (STMG)
Matière	Spécialité SIG (Système d'Information de Gestion)
Thème	L'organisation informatisée.
Question de gestion	Les évolutions technologiques sont-elles exemptes de risques pour l'organisation ?
Notions	• Informatique et innovation technologique • TIC et responsabilités sociales et environnementales des organisations • Risques informatiques • Protection des données : aspects règlementaires, aspects organisationnels, aspects techniques
Mots clés	ENT, évolution technologique, risques technologiques, risques humains, risques organisationnels
Auteurs	Isabelle Pelletier, avec la contribution de Gaëlle Castel
Version	V 1.0

Première partie : Définir l'espace numérique de travail.

1. Ouvrir une session sur l'ENT, relever et définir chacun des services proposés par cet outil en précisant leurs finalités.
2. Pour chacun des services, indiquer ceux que vous utilisez et dans quel contexte.
3. Pour les fonctionnalités ou services que vous n'utilisez pas, rechercher une exploitation possible au sein de la classe.

Deuxième partie : Étudier l'impact de l'ENT sur les modes de travail, de coordination et d'échange entre les différents acteurs.

À l'aide de la vidéo proposée et du dossier documentaire, répondre aux questions suivantes :

4. Retrouver les acteurs internes et externes à l'établissement, qui sont concernés par la mise en place d'un ENT.
5. À partir de la vidéo, expliquer rapidement pour chaque acteur, les avantages que procure la mise en place de l'ENT. Vous remplirez pour cela le tableau suivant :

Acteurs	Avantage

6. Réaliser une interview des différents acteurs afin de de répondre, pour chacun d'entre eux, aux questions suivantes :
   - Quelles sont les fonctionnalités utilisées ?
   - Quelles évolutions sont constatées sur leur mode de travail, de coordination et d'échange avec les autres acteurs.
   - Quels sont les avantages et les limites liés à l'usage d'un ENT ?

Troisième partie : Quels sont les risques liés à la mise en place d'un ENT dans un établissement scolaire ? Quelles sont les solutions pour s'en prémunir ?

À l'aide du document 1 et du site de la CNIL, répondre aux questions suivantes :

7. Rappeler le rôle de la CNIL.
8. Définir ce qu'est une donnée à caractère personnel. Identifier le(s) responsable(s) du traitement de ces données.

9. Retrouver les principaux éléments de droit de la loi « Informatique et libertés ».
10. Relever et définir les différents principes de la protection des données personnelles.
11. Expliquer pourquoi la mise en place d'un ENT doit respecter la loi « Informatique et libertés ».
12. Indiquer les dispositions que doit prendre le chef d'établissement pour respecter les recommandations de la CNIL.

À l'aide des documents 1, 2 et de vos recherches sur internet, répondre aux questions suivantes :

13. Donner une définition des mots suivants : authentification, autorisation, SSO (*Single Sign-On*).
14. Définir l'expression suivante : « Un service de propagation de l'identité ».
15. Représenter sous la forme d'un schéma, le processus qui permet à un utilisateur de se connecter à l'ENT.
16. Identifier et expliciter rapidement les différentes preuves d'authentification citées par le ministère de l'Éducation nationale.
17. Déterminer si le cahier des charges réalisé par le ministère de l'Éducation nationale répond aux recommandations définies par la CNIL concernant la protection des données personnelles.

Le dossier documentaire

Document 1 Les recommandations de la CNIL

La CNIL a rendu son avis le 27 avril[1] sur la mise en place des espaces numériques de travail au sein des établissements scolaires et universitaires. La Commission considère que la mise en œuvre des ENT doit contribuer à la sensibilisation des enseignants, des élèves et de leurs parents aux principes de la protection des données à caractère personnel.

La CNIL a été saisie par le Ministère de l'éducation nationale d'une demande d'avis sur la mise en place au sein des établissements scolaires et universitaires d'espaces numériques de travail (ENT). Considérés comme des téléservices de l'administration électronique, les ENT, parfois aussi appelés «cartable électronique», «cartable numérique» ou «bureau virtuel» sont des sites web portail permettant aux élèves et à leurs parents, aux étudiants, aux enseignants, aux personnels administratifs et plus généralement à tous les membres de la communauté éducative, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques (accès à des contenus à vocation pédagogique et éducative, diffusion d'informations administratives ou relatives à la vie scolaire et au fonctionnement de l'établissement). […]

Dès lors, chaque chef d'établissement est considéré comme responsable des traitements mis en œuvre dans le cadre d'un ENT et doit les déclarer auprès de la CNIL. Afin de leur simplifier cette démarche, un acte réglementaire unique, en l'espèce un arrêté, a été adopté par le Ministère de l'éducation nationale. Chaque responsable d'établissement devra adresser à la CNIL un engagement de conformité s'il a fait le choix de créer un ENT qui rentre dans le cadre fixé par le ministère. Cette déclaration l'engagera à respecter les dispositions prévues dans l'arrêté et notamment les finalités, les droits des personnes et les mesures de sécurité nécessaires à la protection de données à caractère personnel. Lors de l'examen de ce dossier, la CNIL a tout particulièrement porté son attention sur les mesures prises pour assurer la sécurité du dispositif. Celles-ci doivent notamment garantir que chaque titulaire d'un compte ENT ne puisse accéder qu'aux seules informations le concernant (exemple : un parent d'élève ne peut avoir accès qu'aux seules informations relatives à la vie scolaire de son enfant telles les notes, les absences, le cahier de textes de la classe). À cet égard, la CNIL a appelé l'attention des responsables d'établissement sur la nécessité de sensibiliser les utilisateurs des ENT aux mesures élémentaires de sécurité telles que la non-divulgation de leur identifiant de connexion à leur compte ENT. Par ailleurs, s'agissant de l'information des personnes, la CNIL a, dans son avis, rappelé l'obligation faite à chaque responsable d'établissement d'informer les utilisateurs des ENT sur leurs droits au regard de la loi informatique et libertés. Cette information doit être prévue sur la page d'accueil du portail ENT et lors de la phase de création d'un compte ENT.

http://www.cnil.fr/la-cnil/actualite/article/article/lavis-de-la-cnil-sur-les-espaces-numeriques-de-travail-ent-dans-le-systeme-educatif/

[1] NDLR : 27 avril 2006

Document 2 Extrait du Schéma directeur des espaces numériques de travail (SDET) - Recommandations pour l'Authentification-Autorisation-SSO (AAS) - Ministère de l'éducation nationale

Le Schéma Directeur des Espaces numériques de Travail (SDET) 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.

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 :

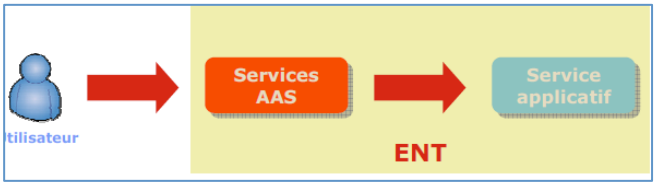
- S'assurer que les services applicatifs disponibles depuis l'ENT pourront utiliser les services AAS pour sécuriser, contrôler ces accès.
- Permettre l'interopérabilité entre les services AAS concourant à la sécurisation de l'accès aux services applicatifs.
- Permettre l'accès aux Téléservices de l'Education Nationale ainsi qu'aux autres services applicatifs distants (notamment les services tiers fournisseurs de ressources pédagogiques).

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 […].

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'utilisateur à un service applicatif.



Les services AAS comportent obligatoirement

- Un service d'identification/d'authentification ;
- Un service de propagation de l'identité ;
- Un service d'autorisation.

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'identités 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. […]

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.

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). […]

Les moyens d'authentification

L'authentification d'un utilisateur DOIT reposer sur la vérification d'un 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. […]

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.

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.

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.

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.

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.