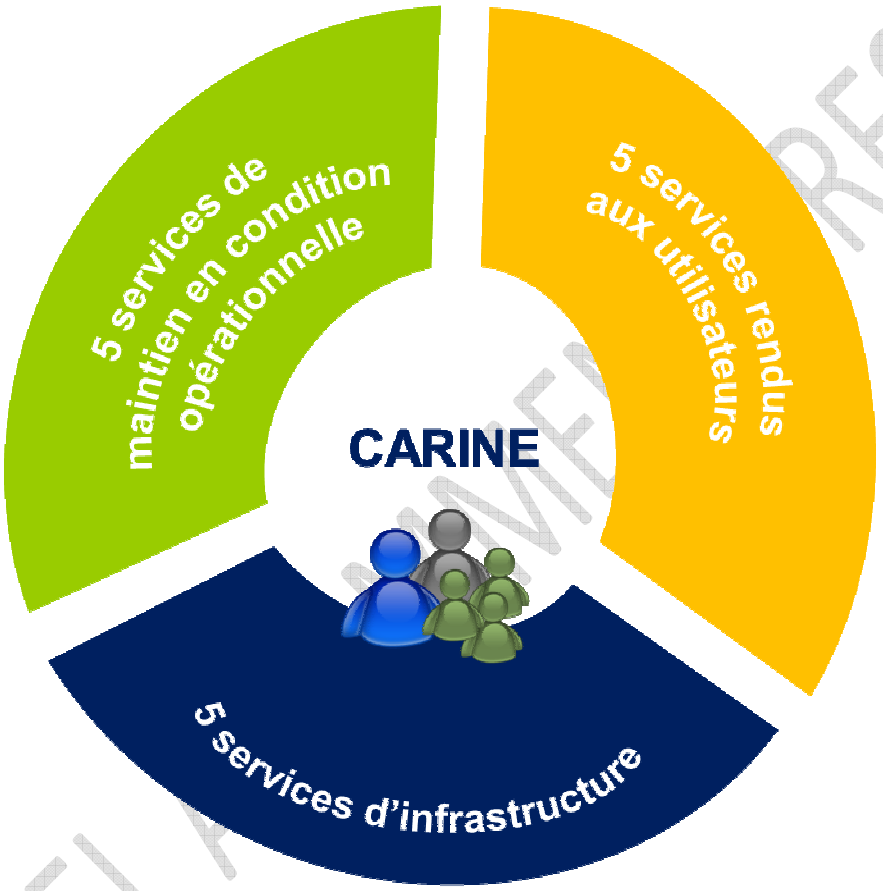
CADRE DE REFERENCE

DES SERVICES

D'INFRASTRUCTURES NUMERIQUES D'ETABLISSEMENTS SCOLAIRES ET D'ECOLES



APPEL A COMMENTAIRES

Document de travail

Statut : Appel à commentaires
Version : v0.15

Niveau de confidentialité : Diffusion pour appel à commentaires

Sommaire

1. OBJET DU DOCUMENT 4
2. PÉRIMÈTRE, ORIENTATIONS ET CIBLE DES SERVICES D'INFRASTRUCTURES NUMÉRIQUES 6
2.1 PRÉSENTATION DES 15 SERVICES 6
2.2 LES CAS D'UTILISATION DU RÉFÉRENTIEL 8
2.2.1 CAS D'USAGE N°1 : RÉFLEXION TERRITORIALE 8
2.2.2 CAS D'USAGE N°2 : RÉFLEXION LOCALE 9
2.2.3 CAS D'USAGE N°3 : RÉDACTION D'UN APPEL D'OFFRES 9
2.2.4 CAS D'USAGE N°4 : DÉPLOIEMENT DES SERVICES NUMÉRIQUES 10
2.2.5 CAS D'USAGE N°5 : SUPERVISION, EXPLOITATION ET ACCOMPAGNEMENT DES UTILISATEURS 10
3. RÉFÉRENCES DES SERVICES 11
3.1 STRUCTURE DES FICHES SERVICES 11
3.2 SERVICES D'INFRASTRUCTURE 12
3.2.1 SERVICE D'ANNUAIRE 12
3.2.2 SERVICE POSTE DE TRAVAIL 16
3.2.3 LE SERVICE D'AUTHENTIFICATION 20
3.2.4 SERVICE DE SÉCURITÉ ET D'ACCÈS RÉSEAU 24
3.2.5 SERVICE DE DIFFUSION D'INFORMATION 29
3.3 SERVICES DE MAINTIEN EN CONDITION OPÉRATIONNELLE 32
3.3.1 SERVICE DE SAUVEGARDE 32
3.3.2 SERVICE DE RÉGÉNÉRATION ET DE CONFIGURATION DE STATIONS 36
3.3.3 SERVICE DE SUPERVISION ET D'EXPLOITATION DE L'INFRASTRUCTURE 39
3.3.4 SERVICE DE GESTION DES JOURNAUX 42
3.3.5 SERVICE DE GESTION DE PARC 46
3.4 SERVICES AUX UTILISATEURS 50
3.4.1 SERVICE DE STOCKAGE 50
3.4.2 SERVICE DE MESSAGERIE ÉLECTRONIQUE 54
3.4.3 SERVICE DE COMMUNICATION TEMPS RÉEL 58
3.4.4 SERVICE DE PUBLICATION 61
3.4.5 SERVICE DE RECHERCHE DOCUMENTAIRE 64
4. POSITIONNEMENT DANS LE RÉFÉRENTIEL DOCUMENTAIRE 66

APPEL À COMMENTAIRES

5. HISTORIQUE ET PRINCIPALES NOUVEAUTÉS 67

6. ANNEXES 70

6.1 DOCUMENTS DE RÉFÉRENCE 70

6.2 GLOSSAIRE 70

APPEL À COMMENTAIRES

1. Objet du document

Le présent document a pour objet de fournir le **CA**dre de **R**éférence national des services d'**I**nfrastructures **N**umériques d'**É**tablissements scolaires et d'écoles (CARINE). Il annule et remplace la précédente version du cadre de référence des S2i2e de 2008.

Le CARINE constitue le cadre de référence commun aux acteurs décisionnaires des écoles, établissements scolaires, aux inspecteurs d'académie, aux recteurs, aux responsables des collectivités territoriales, ainsi qu'aux éditeurs de solutions et prestataires de services.

Il précise les éléments jugés comme suffisamment importants et structurants pour être portés à l'attention de ces différents acteurs.

Le CARINE doit permettre :

- de faciliter le dialogue entre acteurs pour la mise en œuvre des services,
- de formaliser les exigences en termes de qualité de service attendue,
- de définir les principes et de préciser les règles qui permettront de favoriser l'homogénéité des solutions et des pratiques et de faciliter la mutualisation des ressources,
- de répondre à l'émergence de nouveaux besoins.

Le CARINE est le référentiel maître pour les services d'infrastructure et les services de maintien en condition opérationnelle.

Le CARINE n'est pas le référentiel maître des services rendus aux utilisateurs (ces services sont décrits en détail dans d'autres référentiels comme le SDET). Le CARINE complète ces descriptions portées par d'autres référentiels en y ajoutant les exigences et les contraintes d'infrastructure et de sécurité.

APPEL À COMMENTAIRES

Ce document décrit un certain nombre de recommandations. Dans le respect de ces recommandations, la terminologie définie dans la RFC 2119 est utilisée avec les traductions suivantes :

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

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

1. **DOIT** : ce mot, ou l'adjectif « 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** : ce mot, ou l'adjectif « NON RECOMMANDÉ », signifie que la définition est prohibée. Il peut toutefois exister des raisons valables, dans des circonstances particulières, quand le comportement ainsi défini 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 élément est facultatif. Cela signifie que la présence de l'élément en question améliore le service, mais que son absence n'empêche pas le service d'être rendu.

APPEL À COMMENTAIRES

2. Périmètre, orientations et cible des services d'infrastructures numériques

2.1 Présentation des 15 services

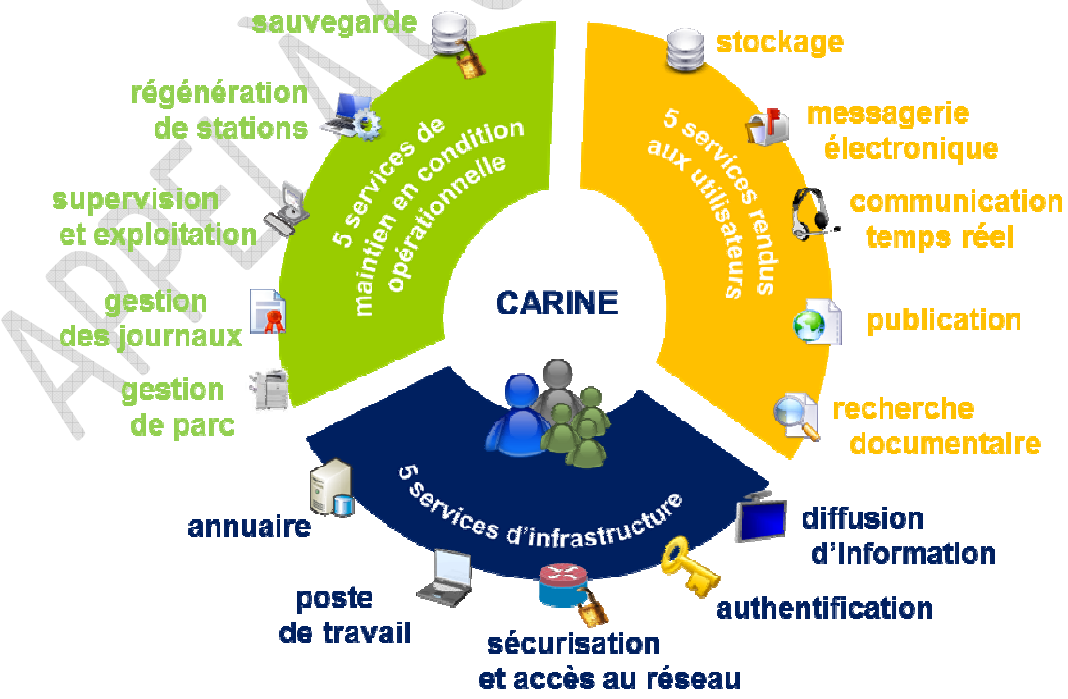
Les Services d'Infrastructures Numériques ont pour objectif principal la fourniture d'un ensemble de services indispensables à l'accès des services de plus haut niveau (tels que les outils de gestion du SI des collèges et des lycées, les ENT ou d'autres services spécifiques à un type d'enseignement, à un environnement local particulier…). Les services de plus haut niveau nécessitent par exemple l'existence du service de sécurisation et d'accès aux réseaux.

Les Services d'Infrastructures Numériques doivent permettre également la communication interne et l'ouverture du SI des collèges, des lycées et des écoles vers l'extérieur dans des conditions de sécurité optimales. C'est pourquoi certains services de haut niveau, rendus aux utilisateurs, sont abordés dans le CARINE, soit de manière transitoire (avant l'arrivée des ENT) ou complémentaire.

Les services hors cadre institutionnels, c'est-à-dire choisis, installés et utilisés par les personnels ou les élèves en établissements/écoles ne sont pas abordés dans le CARINE. Le choix d'installer et d'utiliser des services hors périmètre du CARINE:

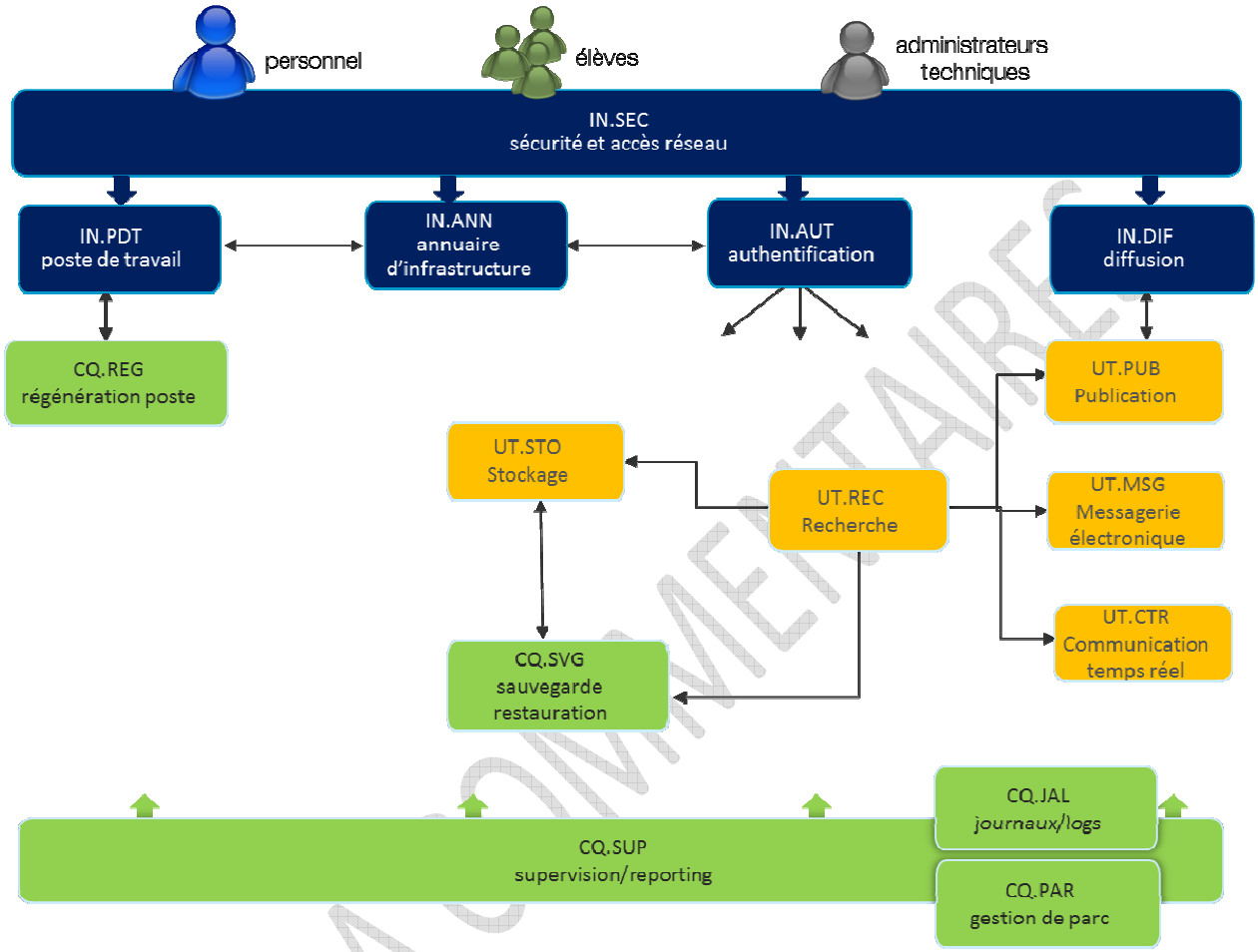
- Par les élèves – est du domaine du choix individuel, DOIT se faire sous l'autorité des parents pour les mineurs. Il n'y a pas de prescription institutionnelle possible.
- Par les personnels – est du domaine du choix individuel. Leur responsabilité est engagée sur les contenus traités.

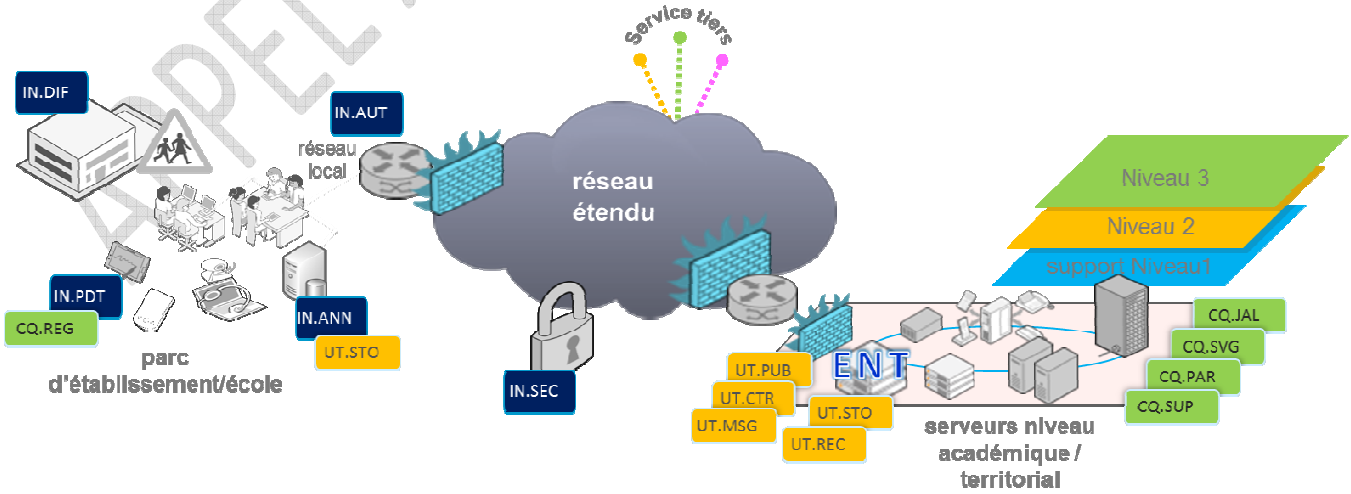
Les Services d'Infrastructures Numériques recouvrent 15 services répartis en 3 catégories :



APPEL A COMMENTAIRES

Les 2 schémas ci-dessous donnent une vue synthétique et très simplifiée des interactions entre les services :

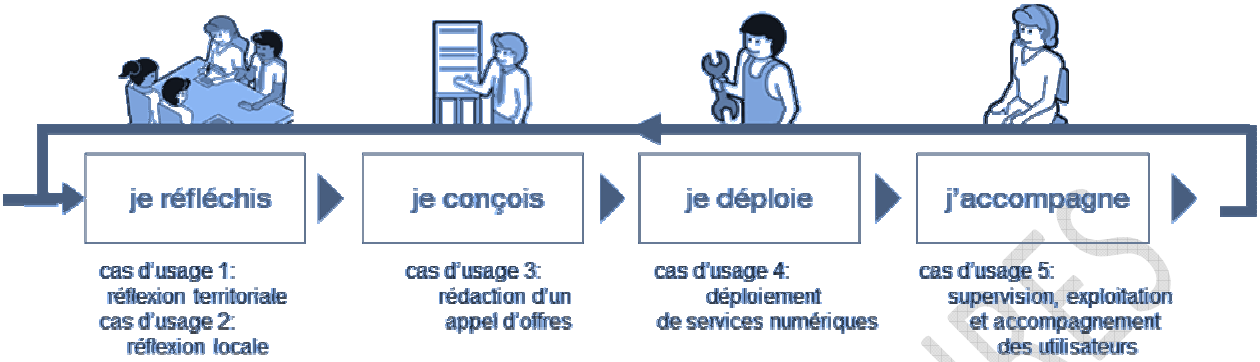




APPEL A COMMENTAIRES

2.2 Les cas d'utilisation du référentiel

Le CARINE peut être utile à chaque grande étape du cycle de vie d'un projet numérique en environnement scolaire, du cadrage de la stratégie à la gestion opérationnelle. Pour illustrer cette dimension temporelle des projets, 5 cas d'usage ont été définis :



Tous les acteurs concernés par les Services d'Infrastructures Numériques dans les établissements scolaires et les écoles ne sont pas tous mobilisés sur chacun de ces cas d'usage. Toutefois, dans un objectif d'efficience et de qualité du service rendu, il est indispensable d'avoir une vision globale des sujets abordés :

- Un acteur mobilisé sur les phases amonts de stratégie et de réflexion doit anticiper la faisabilité et l'exploitabilité des scénarios envisagés ;
- Un acteur mobilisé sur les phases aval de déploiement et d'accompagnement doit comprendre les objectifs et les enjeux associés au service mis en œuvre.

2.2.1 Cas d'usage n°1 : réflexion territoriale

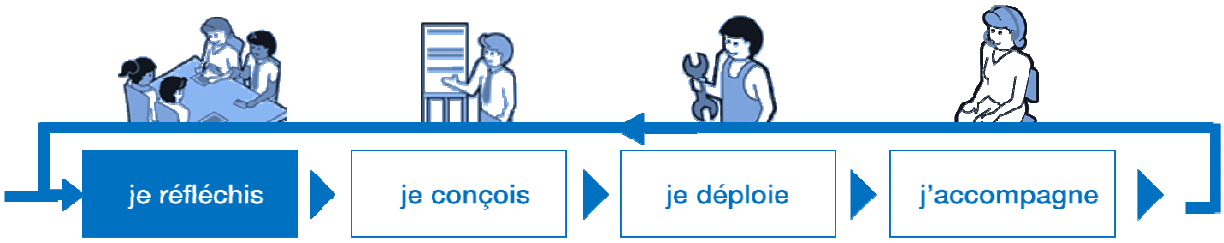
En prévision d'une réunion de coordination sur la politique numérique éducative entre le rectorat et les collectivités, vous avez besoin, en préparation de votre réunion, d'identifier les besoins, moyens et préconisations liés aux infrastructures numériques.

Dans ce contexte, le CARINE peut vous aider à construire vos argumentaires sur des sujets tels que:

- Raccordement d'un établissement/d'une école au haut-débit
- Déploiement d'une infrastructure Wi-Fi dans un établissement/une école
- Qualification des besoins métier (pédagogie, gestion)
- Définition des modalités d'hébergement des services
- Équipement en terminaux fixes et mobiles
- Prise en compte des équipements personnels (BYOD)
- Catalogues des services / outils logiciels requis (pédagogiques et administratifs)
- Catalogues des services / outils logiciels conseillés et optionnels

APPEL À COMMENTAIRES

2.2.2 Cas d'usage n°2 : réflexion locale



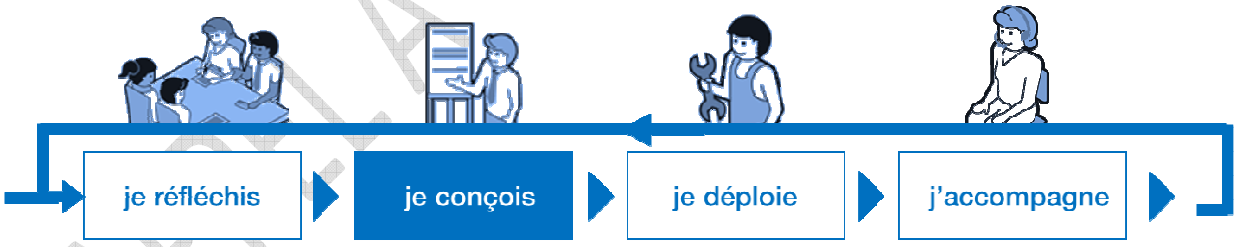
Dans le cadre de la stratégie numérique mise en place par la collectivité et le rectorat, vous êtes amené :

- En tant que chef d'établissement, directeur d'école ou IEN de circonscription, à formaliser des besoins métiers (pédagogie, gestion) en prévision de l'intégration de services numériques dans votre établissement,
- En tant que porteur des sujets numériques en collectivité ou dans un rectorat, à arbitrer sur les projets à mettre en œuvre en fonction de la stratégie définie et des capacités techniques requises.

Dans ce contexte, le CARINE peut vous aider à construire vos argumentaires sur des sujets tels que:

- Équipement en terminaux fixes ou mobiles
- Prise en compte des équipements personnels (BYOD)
- Catalogue des services / outils logiciels requis (pédagogiques et administratifs)
- Catalogues des services / outils logiciels conseillés et optionnels

2.2.3 Cas d'usage n°3 : rédaction d'un appel d'offres



Dans le cadre du développement des services numériques dans un établissement/école, vous êtes amené à réaliser des appels d'offres et/ou à faire des choix pour l'acquisition et la mise en œuvre de matériels et services tels que :

- Infrastructures (serveurs, réseau, stockage, réseau sans-fil …)
- Terminaux fixes et mobiles (ordinateurs fixe, ordinateurs portable, ordiphone …) et tout Equipement Individuel Mobile (EIM)
- Services numériques et outils logiciels (suite bureautique, logiciels vidéo, audio…)

Dans ce contexte, le CARINE peut vous aider à construire votre cahier des charges pour la consultation.

A FAIRE COMMENTAIRES

2.2.4 Cas d'usage n°4 : déploiement des services numériques

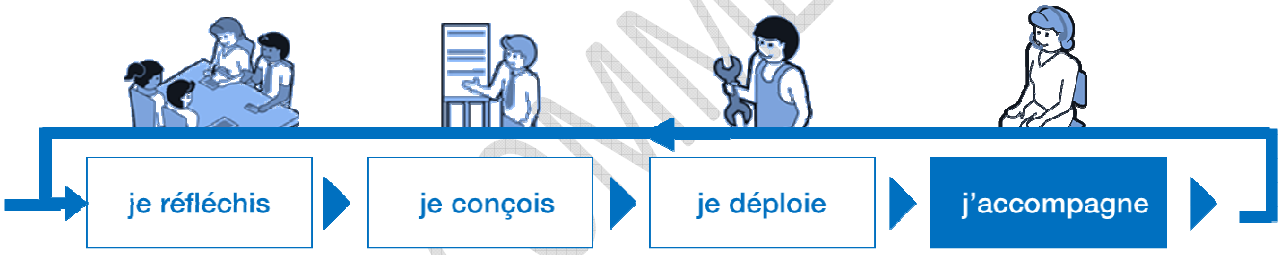
Faisant suite à l'attribution des marchés, la mise en œuvre des services va être initiée en lien avec l'ensemble des parties prenantes :

- Rectorat,
- Etablissements concernés,
- Collectivités de rattachement,
- Prestataires.

Dans ce contexte, afin de préparer l'intégration et le déploiement auprès des utilisateurs de nouveaux matériels et/ou services vous devez traiter en tout ou partie les sujets suivants :

- La qualification des besoins métier (pédagogie, gestion),
- L'intégration de services numériques (hors ENT) dans l'écosystème existant (métier + infrastructures),
- L'intégration d'un ENT dans l'écosystème existant (métier + infrastructures),
- La phase de test et recette de la solution qui valide le déploiement,
- L'exploitation et la maintenance des services numériques.

2.2.5 Cas d'usage n°5 : supervision, exploitation et accompagnement des utilisateurs



Suite à la mise en œuvre d'un service numérique en établissement ou en école, le service passe en phase opérationnelle.

Dans ce contexte, vous pourriez avoir à définir et organiser les tâches suivantes :

- L'accompagnement et le support aux utilisateurs
- La définition des règles d'exploitation et de supervision et la répartition des responsabilités attachées,
- L'exploitation et la maintenance du service numérique.

APPEL À COMMENTAIRES

3. Références des services

3.1 Structure des fiches services

Chaque service est décrit en 2 parties :

- Une fiche synthétique qui donne un aperçu global du service rendu avec :
    - Le besoin ;
    - Les impacts sur les infrastructures ;
    - Les impacts sur l'organisation ;
    - Les impacts sur la sécurité ;
    - Les aspects juridiques importants dont la protection des mineurs ;
    - Les interactions avec les autres services d'infrastructure.
- Un tableau de fonctionnalités qui détaille une à une les fonctionnalités exigées, recommandées et facultatives.

Légende pour la lecture des tableaux de description des services :

Les services du CARINE doivent offrir un certain nombre de fonctions et/ou répondre à des exigences particulières qui sont exprimées dans ces tableaux.

Un service est caractérisé par un code d'identification et un libellé. La mention « *Référentiel maître* » précise le référentiel majeur pour le service considéré. S'il est mentionné autre chose que CARINE, c'est que le service est décrit en détail dans le référentiel mentionné et que le CARINE vient compléter en y ajoutant des contraintes d'infrastructure.

Un service regroupe un ensemble de fonctions, déclinées en fonctionnalités et répondant à certaines règles. Ces fonctions sont détaillées sous forme de tableaux.

Trois niveaux de préconisation s'appliquent aux fonctionnalités :

- Le niveau « E-exigé », appliqué à une fonctionnalité et/ou règle de gestion, signifie que le service correspondant DOIT offrir ladite fonctionnalité.
- Le niveau « R-recommandé », appliqué à une fonctionnalité et/ou règle de gestion, signifie que le service correspondant DEVRAIT offrir ladite fonctionnalité. La décision de ne pas fournir la fonctionnalité ou de ne pas respecter la règle de gestion doit être pesée dans toutes ses conséquences (pédagogique, administrative, juridique et/ou organisationnelle) et dument justifiée auprès des acteurs concernés.
- Le niveau « F-facultatif » appliqué à une fonctionnalité et/ou règle de gestion, signifie qu'il est souhaitable d'appliquer cette recommandation mais qu'il peut exister des éléments de contexte rendant son application difficilement réalisable ou disproportionnée par rapport aux enjeux et aux objectifs prioritaires assignés au projet.

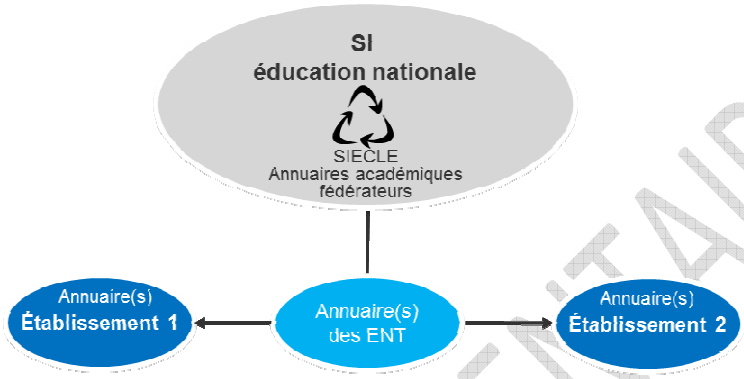
APPEL A COMMENTAIRES

3.2 Services d'infrastructure

3.2.1 Service d'annuaire

Service d'annuaire

Du fait de la responsabilité juridique liée à la fourniture d'accès au réseau et à internet ainsi qu'au caractère personnel de certaines données, tout utilisateur DOIT être identifié et authentifié (voir **service d'authentification<IN.AUT>)** de façon unique avant d'accéder aux ressources. Cela nécessite la mise en œuvre d'annuaires d'identités (annuaires académiques, annuaires ENT) et d'annuaires d'infrastructure en établissement/école.



Impacts sur les infrastructures

Le service d'annuaire d'infrastructure de l'établissement ou de l'école, fournit un référentiel qui permet l'identification des utilisateurs dans le but de contrôler l'accès aux terminaux informatiques et aux réseaux, de gérer et personnaliser ces terminaux et leurs applications et de permettre une gestion adaptée de l'accès aux services locaux (serveurs de fichiers, imprimantes…).

Processus d'échange : L'annuaire ENT est alimenté automatiquement et régulièrement à partir de l'annuaire académique fédérateur (AAF), lui-même alimenté à partir des bases de gestion (SIECLE, STSWEB, BE1D…), en ce qui concerne les élèves, les parents et tous les personnels affectés à l'établissement/école.

Processus d'interrogation : Le service d'annuaire DOIT offrir des mécanismes standard (LDAP) d'interrogation et de recherche (requêtes) sur les annuaires d'infrastructure d'établissements/d'écoles.

Processus d'import/export : Le service d'annuaire DOIT offrir des mécanismes standard (LDAP) d'import/export (réplication/synchronisation) pour permettre l'alimentation des annuaires d'infrastructure d'établissements/d'écoles à partir d'un annuaire académique (solution cible du ministère à terme) ou de celui de l'ENT (voir **annexe Annuaire du SDET**). Cette synchronisation entre annuaires DOIT être sécurisée (réalisée dans une zone sécurisée et/ou via des échanges sécurisés).

Impacts sur l'organisation

Les processus d'échange entre les annuaires académiques, les bases de gestion, l'annuaire ENT et les annuaires d'infrastructures d'établissement/d'école sont définis par le ministère.

Les éventuels besoins d'interaction avec les annuaires des collectivités territoriales doivent être étudiés en collaboration avec ces dernières, dans l'objectif de permettre l'interopérabilité des systèmes d'information, tout en respectant la loi n° 78-17 du 6 janvier 1978..

La personne responsable des traitements de données à caractère personnel contenues dans les annuaires d'infrastructure peut déléguer tout ou partie de la responsabilité opérationnelle à une ou des personnes identifiées de manière claire (information des personnes concernées par les traitements).

Impacts sur la sécurité des SI

En établissement/école, le référentiel d'identité maître est l'annuaire ENT. L'annuaire ENT DOIT être le seul annuaire contenant les données d'identité détaillée des utilisateurs pour l'établissement/école (hormis la base de gestion SIECLE, accessible uniquement depuis la zone « administrative »).

Les flux d'alimentation et de réplication des annuaires ne DOIVENT transiter que sur des réseaux sécurisés ou via des protocoles chiffrés.

Toute modification ou tentative de modification d'un annuaire DOIT être tracée, identifiée et horodatée. (voir **service de**

APPEL A COMMENTAIRES

gestion des journaux <CQ.JAL>)

Aspects juridiques

La constitution d'un annuaire sur support informatisé comportant l'identité des personnes, leur fonction, leurs coordonnées professionnelles et le cas échéant leur photographie, constitue un traitement de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée en 2004.

Les annuaires d'infrastructure PEUVENT être alimentés à partir de l'annuaire ENT ou d'un annuaire académique (solution cible du ministère à terme) mais ne DOIVENT reprendre que les données strictement nécessaires à leurs fonctions.

Les annuaires d'infrastructure contiennent des données à caractère personnel. Le chef d'établissement / l'IEN est responsable de ces données sur le périmètre de son établissement / de sa circonscription.

Certains annuaires peuvent stocker des données à caractère personnel sensibles (données de santé par exemple) ou des images (photos d'identité par exemple). Ces données sont couvertes par des dispositions légales particulières concernant les données de santé et le droit à l'image. (voir **service de stockage <UT.STO>)**

Les annuaires d'infrastructure ne DOIVENT contenir que les données strictement indispensables à leurs fonctions. Un transfert exhaustif d'un annuaire ENT ou académique NE DOIT PAS être autorisé.

Consulter régulièrement la rubrique « éducation » sur le site de la CNIL et contrôler le niveau de conformité de l'établissement ou de l'école avec les fiches pratiques diffusées sur www.cnil.fr.

http://eduscol.education.fr/internet-responsable/textes-legislatifs-et-reglementaires.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/image-et-video.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
IN.ANN.1	Identification	Tout utilisateur DOIT être identifié (via le service d'annuaire) et authentifié (via le **service d'authentification)** avant l'accès aux ressources.	E	E
IN.ANN.2	Requêtes	Le service d'annuaire DOIT offrir des mécanismes standard (LDAP) d'interrogation et de recherche (requêtes) sur les annuaires d'infrastructure d'établissements/d'écoles.	E	E
IN.ANN.3	Alimentation	Le service d'annuaire DOIT offrir des mécanismes standard (LDAP) d'import/export (réplication/synchronisation) pour permettre l'alimentation des annuaires d'infrastructure d'établissements/d'écoles à partir d'un annuaire académique (solution cible du ministère à terme) ou de celui de l'ENT.	E	E
IN.ANN.4	Traçabilité	Toute modification ou tentative de modification d'un annuaire DOIT être tracée, identifiée et horodatée.	E	E
IN.ANN.5	Import/Export	Les flux d'alimentation et de réplication des annuaires ne DOIVENT transiter que sur des réseaux sécurisés ou via des protocoles cryptés.	E	E
IN.ANN.6	Import/Export	Les annuaires d'infrastructure PEUVENT être alimentés à partir de l'annuaire ENT ou d'un annuaire académique (solution cible du ministère à terme) mais ne DOIVENT reprendre que les données strictement nécessaires à leurs fonctions.	E	E
IN.ANN.7	Contenu	Les annuaires d'infrastructure ne doivent contenir que les données strictement indispensables à leurs fonctions. Un transfert exhaustif d'un annuaire ENT ou académique NE DOIT PAS être autorisé.	E	E

IN.ANN.8	Contenu	En établissement/école, le référentiel d'identité maître est l'annuaire ENT. L'annuaire ENT DOIT être le seul annuaire contenant les données d'identité détaillée des utilisateurs pour l'établissement/école (hormis la base de gestion SIECLE, accessible uniquement depuis la zone « administrative » des EPLE).	E	E

APPEL À COMMENTAIRES

3.2.2 Service poste de travail

Service poste de travail

L'utilisateur accède aux services numériques à l'aide d'un poste de travail, qui peut être fixe ou mobile.

*Pour les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur les infrastructures

Le service poste de travail fournit le ou les terminaux permettant l'accès aux services numériques. Cela inclut les postes fixes et mobiles.

Type de poste : Les postes de travail PEUVENT être en configuration client lourd (poste classique avec son stockage et ses applications), client léger (données et applications distantes), voire ultra léger/zéro client (mode terminal passif).

Si elles sont utilisées, les techniques de déport des applications (virtualisation d'application) DOIVENT tenir compte des contraintes de débit réseau et des impacts sur l'infogérance (gestion des accès, des serveurs de distribution, des impressions…).

Configuration du poste : Dans un objectif de qualité de service, de sécurité et de simplification de l'infogérance, les configurations des postes de travail DEVRAIENT être « masterisées ». Lorsque les débits réseau le permettent, les techniques utilisées devraient privilégier les outils de télédistribution à distance. (voir **service de régénération de configuration <CQ.REG>**)

Les personnes handicapées DOIVENT être équipées de postes adaptés.

http://eduscol.education.fr/cid56843/ressources-numeriques-adaptees-soutenues-et-realisees.html

Impacts sur l'organisation

La typologie des postes de travail doit être définie par le ministère en collaboration avec les collectivités territoriales. Cette typologie doit correspondre au profil des utilisateurs (personnels, élèves), à leur usage (pédagogie et/ou gestion) et à leur situation d'usage (fixe, mobilité).

Lien vers le référentiel « matériel et organisation des TICE » < http://eduscol.education.fr/cid57393/referentiels-d-equipement-ecole-et-college.html>

Un poste de travail peut contenir des données personnelles, voire privées, d'un utilisateur. L'utilisateur DOIT identifier ces données en les marquants par les mots "PERSONNEL" ou "PRIVÉ" (voir **service de stockage <UT.STO>**).

Les utilisateurs doivent être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. (Cf. recommandations et fiches pratiques CNIL : http://www.cnil.fr/les-themes/scolarite-mineurs/article/article/10-conseils-pour-la-securite-de-votre-systeme-dinformation)

Les postes de travail ayant une durée de vie limitée (6 ans en moyenne), leur remplacement et leur mise au rebut devraient être anticipés (voir **service de gestion de parc <CQ.PAR>**).

Les postes des personnels de direction et des gestionnaires doivent pouvoir être remplacés rapidement, notamment en période de rentrée scolaire (ex : provision de postes prêts à l'emploi).

Cela DOIT être également le cas pour les élèves en situation de handicap pour qui l'ordinateur est souvent une prothèse pour appréhender le monde et/ou communiquer.

« BYOD »

APPEL À COMMENTAIRES

Les postes de travail privés des personnels PEUVENT être utilisés dans l'établissement/l'école (BYOD – Bring Your Own Device- ou AVEC en français – Apportez Votre Équipement personnel de Communication). Dans ce cas, la politique de sécurité de l'établissement et le règlement intérieur DEVRAIENT décrire précisément les modalités d'accès ainsi que les limites de responsabilités (ex : assurance, responsabilité juridique vis-à-vis des usages, etc.). Un paragraphe spécifique DEVRAIT également être ajouté à la charte de l'établissement / de l'école (ex : propriété, vie privée, responsabilité juridique vis-à-vis des usages, etc.). (se référer au **dossier BYOD** http://BYOD)

Les élèves en situation de handicap doivent pouvoir utiliser un poste de travail :

- soit notifié par les MDPH et prêté par les académies ;
- soit acheté par les parents.

Ces postes de travail sont souvent équipés de périphériques particuliers : plages braille, claviers spéciaux, dispositifs de pointage adaptés (capteurs), scanners portables, webcams…

Poste partagé

Le partage d'un poste de travail PEUT avoir des impacts sur l'organisation. Dans le cas où le poste est partagé entre plusieurs utilisateurs, le service de régénération et de configuration de stations DEVRAIT être activé. Il est nécessaire de définir clairement les procédures de régénération ou de reconfiguration du poste, la qualité de service attendue (notamment au regard du temps), et le traitement réservé aux données locales. (voir **service de régénération de configuration de stations <CQ.REG>**)

Impacts sur la sécurité des SI

Sécurité du poste : Les postes de travail DOIVENT être sécurisés, c'est à dire a minima imposer une authentification pour l'accès au poste et contenir un antivirus. Ils DEVRAIENT contenir un mécanisme de filtrage des flux (« pare feu individuel »). (voir **service d'authentification<IN.AUT>)**

Les postes de travail DEVRAIENT être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité.

Les postes en libre-service DOIVENT être configurés pour ne donner accès qu'à des services non sensibles. Ces postes NE DOIVENT PAS contenir de données personnelles.

Sécurité des données : Les postes des personnels de direction et des gestionnaires DOIVENT être équipés d'un mécanisme de chiffrement de masse le plus transparent possible pour l'utilisateur.

Droits d'administration : Donner aux utilisateurs les droits administrateurs sur le poste de travail peut avoir des conséquences lourdes sur les processus de maintenance et de maintien en condition opérationnelle. Il faut cependant veiller à ce que les postes utilisés par des personnes en situation de handicap permettent toutes les adaptations nécessaires, notamment la prise en compte de leurs périphériques spécifiques personnels.

Pour permettre l'installation d'outils numériques hors catalogue par les personnels, d'autres solutions PEUVENT être préférées (ex : poste réservé à l'innovation et au test de nouveaux outils, machine virtuelle préinstallée sur le poste…).

Mise au rebut : Lors de la mise au rebut, la récupération puis la suppression définitive des données sur le poste doivent être programmées. Cela peut nécessiter de mettre à disposition temporairement des locaux dédiés à la récupération des anciens postes et à la préparation des nouveaux.

Aspects juridiques

Les élèves en situation de handicap DOIVENT utiliser un poste de travail lors des examens.

http://www.education.gouv.fr/pid285/bulletin_officiel.html?cid_bo=91832

La gestion des déchets (dont la mise au rebut des matériels) est régie par le code de l'environnement, publié pour sa partie législative en annexe de l'Ordonnance n° 2000-914 du 18 septembre 2000 (JO du 21 septembre 2000).

http://eduscol.education.fr/internet-responsable/textes-legislatifs-et-reglementaires.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☒ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☒ gestion de parc	☐ recherche documentaire

APPLICABLE COMMENTAIRES

IN.PDT Service poste de travail	Référentiel maître :CARINE

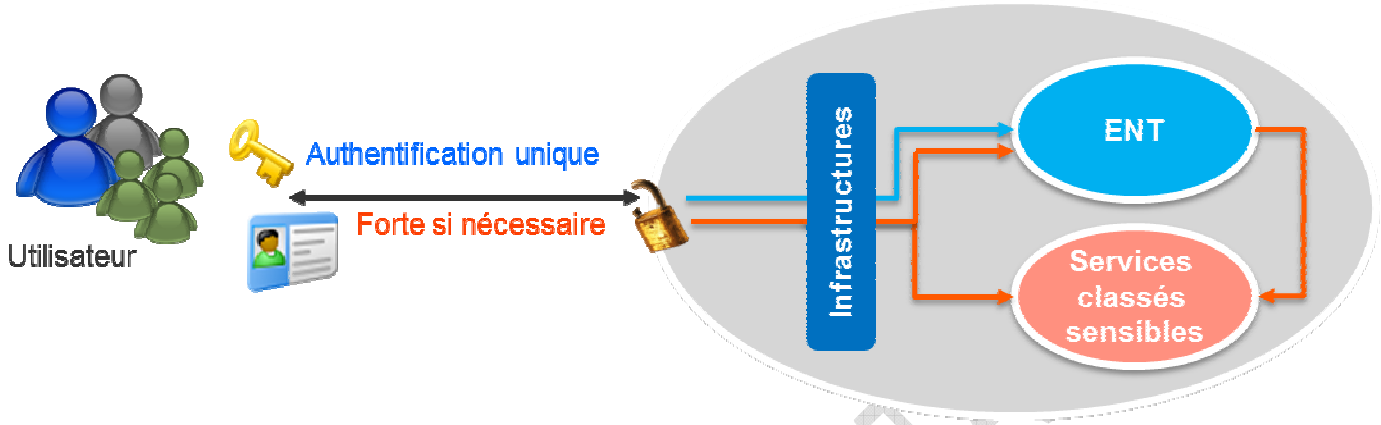
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
IN.PDT.1	Approvisionnement	Les postes des personnels de direction DEVRAIENT être pré-approvisionnés et configurés pour pouvoir être remplacés en une demi-journée. Cela DEVRAIT être également le cas pour les élèves en situation de handicap.	R	R
IN.PDT.2	Configuration	Les postes de travail PEUVENT être en configuration client lourd (poste classique avec son stockage et ses applications), client léger (données et applications distantes), voire ultra léger/zéro client (mode terminal passif).	F	F
IN.PDT.3	Configuration	Dans un objectif de qualité de service, de sécurité et de simplification de l'infogérance, les configurations des postes de travail DEVRAIENT être « masterisées ».	R	R
IN.PDT.4	Stockage	Un poste de travail peut contenir des données personnelles, voire privées, d'un utilisateur. L'utilisateur DOIT identifier ces données en les marquants par les mots "PERSONNEL" ou "PRIVÉ"	E	E
IN.PDT.5	Droits administrateur	Le poste de travail DEVRAIT être fourni configuré de sorte que l'utilisateur n'ait pas les droits d'administration sur le poste.	R	R
IN.PDT.6	Droits administrateur	Pour permettre l'installation d'outils numériques hors catalogue par les personnels, d'autres solutions que celle de donner les droits administrateur à l'utilisateur PEUVENT être préférées (ex : poste réservé à l'innovation et au test de nouveaux outils, machine virtuelle préinstallée sur le poste…).	F	F
IN.PDT.7	Sécurité du poste	L'accès au poste de travail DOIT être soumis à authentification.	R	E

IN.PDT.8	Sécurité du poste	Un antivirus DOIT être installé sur le poste de travail.	E	E
IN.PDT.9	Sécurité du poste	Les postes de travail DEVRAIENT contenir un mécanisme de filtrage des flux (« pare feu individuel »).	R	R
IN.PDT.10	Sécurité	Les postes de travail DEVRAIENT être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité définie dans la politique de sécurité de l'établissement ou de l'école.	R	R
IN.PDT.11	Sécurité des données	Les postes des personnels de direction et des gestionnaires DOIVENT être équipés d'un mécanisme de chiffrement de masse.	E	E
IN.PDT.12	Accessibilité	Les personnes handicapées DOIVENT être équipées de postes adaptés.	E	E
IN.PDT.13	Accessibilité	Les élèves en situation de handicap DOIVENT disposer d'un poste de travail lors des examens.	E	E
IN.PDT.14	Virtualisation	Si elles sont utilisées, les techniques de déport des applications (virtualisation d'application) DOIVENT tenir compte des contraintes de débit réseau et des impacts sur l'infogérance (gestion des accès, des serveurs de distribution, des impressions…).	E	E
IN.PDT.15	AVEC	Les postes de travail privés des personnels PEUVENT être utilisés dans l'établissement/l'école (BYOD – Bring Your Own Device - ou AVEC en français – Apportez Votre Équipement personnel de Communication). Dans ce cas, la politique de sécurité de l'établissement et le règlement intérieur DEVRAIT décrire précisément les modalités d'accès ainsi que les limites de responsabilités (ex : assurance, responsabilité juridique vis-à-vis des usages, etc.). Un paragraphe spécifique DEVRAIT également être ajouté à la charte de l'établissement / de l'école (ex : propriété, vie privée, responsabilité juridique vis-à-vis des usages, etc.).	F R	F R
IN.PDT.16	Partage	Le partage d'un poste de travail peut avoir des impacts sur l'organisation. Dans le cas où le poste est partagé entre plusieurs utilisateurs, le service de régénération et de configuration de stations DEVRAIT être activé. Il est nécessaire de définir clairement les procédures de régénération ou de reconfiguration du poste, la qualité de service attendue (notamment au regard du temps), et le traitement réservé aux données locales.	R	R
IN.PDT.17	Poste en libre-service	Les postes en libre-service DOIVENT être configurés pour ne donner accès qu'à des services non sensibles. Ces postes NE DOIVENT PAS contenir de données personnelles.	E	E

3.2.3 Le service d'authentification

Service d'authentification

Du fait de la responsabilité juridique liée à la fourniture d'accès au réseau et à internet ainsi qu'au caractère personnel de certaines données, tout utilisateur DOIT être identifié (voir **service d'annuaire <IN.ANN>)** et authentifié de façon unique avant d'accéder aux ressources. Cela nécessite la mise en œuvre de mécanismes d'authentification en établissement/école.



Tout utilisateur, et donc tout élève, dispose de moyens d'authentification propres et dont il est responsable.

Impacts sur les infrastructures

L'authentification, parce qu'elle fait partie du processus de contrôle d'accès aux services, DOIT se faire au plus près de l'utilisateur notamment pour permettre l'accès aux ressources locales en toutes circonstances.

Authentification simple : Tout accès aux ressources, internes ou externes, DOIT être soumis à authentification.

Authentification renforcée : Certains utilisateurs PEUVENT utiliser un moyen d'authentification forte pour accéder à une ressource sensible. Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.

Multiplicité des authentifications : Il est important d'appréhender l'authentification de façon unifiée, qu'il s'agisse de l'accès au terminal, de l'accès au réseau local, de l'accès à l'ENT et à ses services tiers* (accès par login/mot de passe), ou de l'accès à d'autres services* dont certains peuvent être des services sensibles (réauthentification ou authentification forte).
**inclut les téléservices*
Le mécanisme d'authentification unique (SSO = Single Sign On) DEVRAIT être mis en oeuvre. Pour les services plus sensibles, deux gradations sont possibles : réauthentification, puis authentification forte. Le SSO DOIT donc préserver la distinction entre authentifications faible et forte en propageant la méthode d'authentification employée.

Postes partagés :Un mécanisme permettant de repérer visuellement et aisément qui est connecté sur le terminal DEVRAIT être présent.

Le service d'authentification DOIT être activé quel que soit le terminal utilisé.

*Pour les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur l'organisation

Spécificité 1er degré

L'étape d'authentification peut poser des problèmes de faisabilité pour les plus jeunes élèves du 1er degré. Pour les très jeunes enfants et les non lecteurs, un mode d'authentification simplifié DEVRAIT être envisagé (ex : mise dans l'ordre de 3 ou 4 images).

Dans le cas d'un équipement individuel mobile, des modes de reconnaissance biométriques PEUVENT être utilisés, à la condition que la donnée qui permet la validation de l'accès, soit uniquement stockée dans le terminal et accessible au seul process d'authentification. [*Note : Les aspects juridiques liés à ces pratiques sont en cours d'instruction*.]

L'authentification DEVRAIT être systématique, notamment pour son intérêt pédagogique.

Les chefs d'établissement/directeurs d'école organisent l'attribution des moyens d'authentification aux utilisateurs de leur établissement/école et/ou veillent à leur bonne utilisation.

Les règles de partage des postes des élèves en situation de handicap avec les AVS/AESH DOIVENT être définies dans la charte de l'établissement ou de l'école.

APPEL A COMMENTAIRES

Les administrateurs techniques ont un accès « super utilisateur » sur de nombreux services d'infrastructure. Cela leur donne des droits et des devoirs particuliers qui DEVRAIENT être formalisés dans une Charte administrateur technique.

Le respect et la bonne gestion d'un service d'authentification (en particulier la gestion des mots de passe) DOIT s'accompagner d'une sensibilisation des utilisateurs sur leur responsabilité.

Chaque utilisateur DOIT s'engager à ne pas divulguer ses mots de passe à d'autres utilisateurs et à ne pas utiliser un autre code utilisateur.

Le rythme de changement des mots de passe DOIT être défini dans la politique de sécurité de l'établissement ou de l'école.

Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DEVRAIT être indiqué dans les conditions d'utilisation des services.

Impacts sur la sécurité des SI

L'authentification simple repose souvent sur la saisie d'un login et d'un mot de passe dont les caractéristiques (longueur et composition) DOIVENT être définies dans la politique de sécurité de l'établissement ou de l'école et rappelées dans les conditions d'utilisation des services.

Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.

Une fois distribués aux utilisateurs, les mots de passe DOIVENT être changés dès la première connexion.

Les mots de passe ne DOIVENT jamais être stockés en clair que ce soit sous forme numérique ou sur papier.

Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DOIT être spécifié dans la politique de sécurité de l'établissement ou de l'école. Toute tentative d'authentification, réussie ou échouée, DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux <CQ.JAL>)**

Aspects juridiques

Le développement d'Internet a profondément modifié la notion même d'identité. D'une identité classiquement vue comme unique, celle de notre état civil, nous sommes passés aujourd'hui à des identités numériques plurielles. Nous pouvons ici apparaître sous notre « vrai nom », là sous un pseudonyme, un avatar, ici encore sous un simple numéro. Ce développement des identités numériques s'est accompagné rapidement d'une nouvelle forme de fraude : l'usurpation d'identité.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/identites-numeriques-et-usurpation-didentite.html

La CNIL donne des recommandations pour la constitution et la gestion des mots de passe :

http://www.cnil.fr/linstitution/actualite/article/article/securite-comment-construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces/

Interaction avec d'autres services

☒ annuaire	☐ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
IN.AUT.1	Authentification	Tout utilisateur DOIT être identifié (via le service d'annuaire) et authentifié avant l'accès à toute ressource locale et/ou distante. L'authentification, parce qu'elle fait partie du processus de contrôle d'accès aux services, DOIT se faire au plus près de l'utilisateur notamment pour permettre l'accès aux ressources locales en toutes circonstances. Le service d'authentification DOIT être activé quel que soit le terminal utilisé. *L'étape d'authentification peut poser des problèmes de faisabilité pour les plus jeunes élèves du 1er degré. Pour les très jeunes enfants et les non lecteurs, un mode d'authentification simplifié DOIT être envisagé (ex : mise dans l'ordre de 3 ou 4 images). L'authentification DEVRAIT être systématique, notamment pour son intérêt pédagogique.	R*	E
IN.AUT.2	Authentification forte	Certains utilisateurs PEUVENT utiliser un moyen d'authentification forte pour accéder à une ressource sensible. Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.	F	F
IN.AUT.3	Authentification unique (SSO)	Un mécanisme d'authentification unique (SSO = Single Sign On) DEVRAIT être mis en oeuvre. Pour les services plus sensibles, deux gradations sont possibles : réauthentification, puis authentification forte. Le SSO DOIT donc préserver la distinction entre authentifications faible et forte en propageant la méthode d'authentification employée.	R	R
IN.AUT.4	Postes partagés	Un mécanisme permettant de repérer visuellement et aisément qui est connecté sur le terminal DEVRAIT être présent.	R	R
IN.AUT.5	Administrateurs techniques	Les administrateurs techniques ont un accès « super utilisateur » sur de nombreux services d'infrastructure. Cela leur donne des droits et des devoirs particuliers qui DEVRAIENT être formalisés dans	R	R

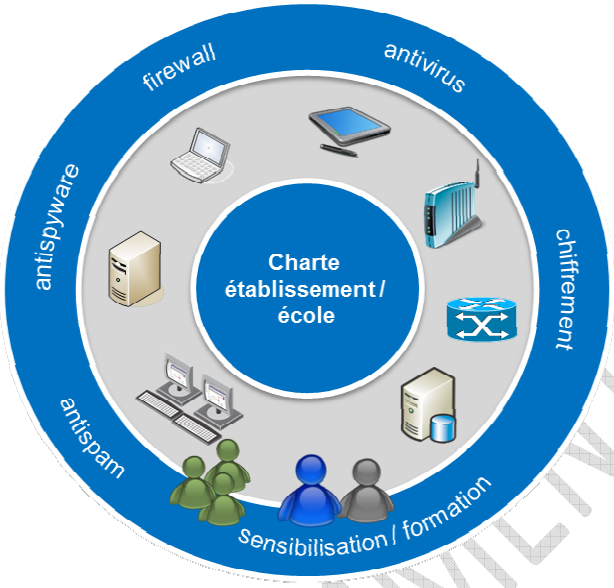
		une Charte administrateur technique.		
IN.AUT.6	Formation/Sensibilisation	Le respect et la bonne gestion d'un service d'authentification (en particulier la gestion des mots de passe) DOIT s'accompagner d'une sensibilisation des utilisateurs sur leur responsabilité.	E	E
IN.AUT.7	Mots de passe	L'authentification simple repose souvent sur la saisie d'un login et d'un mot de passe dont les caractéristiques (longueur et composition) DOIVENT être définies dans la politique de sécurité de l'établissement ou de l'école et rappelées dans les conditions d'utilisation des services.	E	E
IN.AUT.8	Mots de passe	Chaque utilisateur DOIT s'engager à ne pas divulguer ses mots de passe à d'autres utilisateurs et à ne pas utiliser un autre code utilisateur.	E	E
IN.AUT.9	Mots de passe	Une fois distribués aux utilisateurs, les mots de passe DOIVENT être changés dès la première connexion.	E	E
IN.AUT.10	Mots de passe	Le rythme de changement des mots de passe DOIT être défini dans la politique de sécurité de l'établissement ou de l'école.	E	E
IN.AUT.11	Mots de passe	Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DOIT être spécifié dans la politique de sécurité de l'établissement ou de l'école.	E	E
IN.AUT.12	Mots de passe	Les mots de passe ne DOIVENT jamais être stockés en clair que ce soit sous forme numérique ou sur papier.	E	E
IN.AUT.13	Mots de passe	Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DOIT être spécifié dans la politique de sécurité de l'établissement ou de l'école.	E	E
IN.AUT.14	Accessibilité	Les règles de partage des postes des élèves en situation de handicap avec les AVS/AESH DOIVENT être définies dans la charte de l'établissement ou de l'école.	E	E
IN.AUT.15	Biométrie	Dans le cas d'un équipement individuel mobile, des modes de reconnaissance biométriques PEUVENT être utilisés, à la condition que la donnée qui permet la validation de l'accès, soit uniquement stockée dans le terminal et accessible au seul process d'authentification.	F	F
IN.AUT.16	Traçabilité	Toute tentative d'authentification, réussie ou échouée, DOIT être tracée, identifiée et horodatée.	E	E

3.2.4 Service de sécurité et d'accès réseau

Service de sécurisation et d'accès au réseau

L'utilisation des services numériques DOIT se faire dans des conditions de sécurité optimales dont les principes sont définis dans la PSSI de l'établissement ou de l'école et dans le respect de sa charte.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/charte.html



Ces principes visent simultanément à assurer :

- la sécurité du système d'information de l'établissement ou de l'école :
- celle des systèmes d'information tiers auxquels lui-même donne accès ;
- la protection des mineurs dans le cadre de l'utilisation des outils numériques.

Impacts sur les infrastructures

Le service de sécurisation et d'accès au réseau DOIT permettre :

- de sécuriser les postes de travail, fixes ou nomades ainsi que les serveurs ;
  Pour les terminaux mobiles, se référer au ***dossier CARMO <http://CARMO>****.*
- de protéger les données ;
- le filtrage des flux entrants et sortants, en particulier le filtrage des sites web et des flux de communication, dans le cadre de la protection de l'élève mineur ;
- que l'accès aux différents réseaux, filaire ou sans fil (pour le WiFi, se référer au **dossier WiFi <http://dossier WiFi>**), en particulier internet, est réservé aux seules machines autorisées (parc de l'établissement et terminaux personnels enregistrés).

La performance de l'accès aux réseaux (intranet, extranet, internet) a un impact sur l'ensemble des services d'infrastructure et plus largement sur l'ensemble des usages numériques. Un accès performant au réseau DOIT donc être une priorité dans tous les plans d'équipement des établissements/écoles. Les capacités du raccordement à internet, des point d'accès Wi-Fi, des équipements de réseau et de sécurité, et du câblage DOIVENT donc être définis en cohérence pour assurer la meilleure performance.

Point d'attention : avec le développement du très haut débit il est nécessaire d'expertiser les performances du réseau interne de l'établissement ou de l'école afin de tirer parti de l'augmentation du débit externe.

Le service de sécurité est un service transverse dont le niveau global est conditionné par celui de son maillon le plus faible. Tous les services d'infrastructure DOIVENT donc prendre en compte la sécurité afin d'assurer la cohérence et la solidité de la chaîne globale.

Impacts sur l'organisation

La sécurité est l'affaire de tous et repose en grande partie sur la bonne compréhension des responsabilités de chacun et

ADELA COMMENTAIRES

donc sur la sensibilisation des acteurs (personnels, élèves, parents, collectivités territoriales, prestataires). Les principes et les règles DEVRAIENT être décrits aux différents niveaux que constituent la politique de sécurité de l'établissement ou de l'école(ex : distribution et réinitialisation des mots de passe), la charte utilisateur (ex : la non communication de ses moyens d'authentification à des tiers), le règlement intérieur (ex : entrée/sortie des équipements dans l'établissement/école), les conditions générales d'utilisation des équipements (ex : règles de sauvegarde des données situées sur les postes de travail) et/ou dans les contrats de services entre les partenaires (ex : règles d'infogérance).

Filtrage

Les règles de filtrage définis dans les équipements de sécurité, en particulier pour ce qui concerne la protection des mineurs, DOIVENT être sous la responsabilité de l'Education Nationale.

Il est indispensable de distinguer le filtrage des flux (niveaux 2 à 4 du modèle OSI), du filtrage de contenu (web, SMTP, etc.) destiné notamment à assurer la protection des mineurs et le respect des valeurs du service public de l'éducation (neutralité, etc.).

Toutes les méthodes de filtrage PEUVENT être combinées (listes, analyse de contenu…) ; le service ne saurait reposer uniquement sur des listes d'autorisation, sauf contextes particuliers (très jeunes enfants ? épreuves d'examen ?). Ces contextes et les règles applicables DOIVENT être définis par les équipes pédagogiques, hormis le filtrage des contenus manifestement illicites qui est défini au niveau national.

Le service DOIT permettre l'ajout ou le retrait de règles de filtrage de façon simple et adaptée aux personnes autorisées de l'établissement ou de l'école. Le service DEVRAIT proposer un mécanisme de délégation au plus près de l'acte pédagogique.

Le service DEVRAIT être capable de prendre en compte le groupe classe ou le groupe discipline, et d'une façon plus générale tout groupe pédagogique.

Le service DOIT être en mesure d'utiliser les listes de restrictions et d'autorisations actuellement collectées et maintenues par l'université de Toulouse 1.

Chaîne d'alerte : Une chaîne d'alerte et de responsabilités DOIT être mise en place aux niveaux local et académique pour qualifier, investiguer, traiter les incidents. Chacun a un devoir d'alerte, la détection des incidents DOIT donc être l'affaire de tous.

Impacts sur la sécurité des SI

La performance de l'accès aux réseaux (interne, externe) a un impact sur la disponibilité des services d'infrastructure et plus largement sur l'ensemble des usages numériques.

	20 simultanés	50 simultanés	100 simultanés	>100 simultanés
Usages courants	? *À définir*	? *À définir*	? *À définir*	? *À définir*
Usages enrichis (vidéo, son…)	? *À définir*	? *À définir*	? *À définir*	? *À définir*

Aspects juridiques

Protection des mineurs :

Le service de filtrage de contenu (web, SMTP, etc.) est une obligation réglementaire, rappelé par la circulaire N°2004-035 du 18-2-2004 relative à l'usage de l'internet dans le cadre pédagogique et [à la] protection des mineurs) - http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm

Consulter régulièrement les textes sur la protection des mineurs :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

Le chef d'établissement/l'IEN de circonscription est responsable du traitement des données à caractère personnel, des contenus publiés, des usages des services, de la protection des mineurs…

http://www.education.gouv.fr/cid3946/guide-juridique-du-chef-d-etablissement.html

http://www.cnil.fr/linstitution/actualite/article/article/traitements-de-gestion-scolaire-quelles-formalites-cnil-pour-les-chefs-detablissements/

AVEC COMMENTAIRES

http://eduscol.education.fr/internet-responsable/ressources/legamedia/filtrage.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☒ régénération de configurations	☒ messagerie électronique
☒ authentification	☒ supervision et exploitation	☒ communication temps réel
☐ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☒ diffusion d'information	☒ gestion de parc	☒ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
IN.SEC.1	Périmètre	Le service de sécurisation et d'accès au réseau DOIT permettre : ▪ de sécuriser les postes de travail, fixes ou nomades, ainsi que les serveurs ; ▪ de protéger les données ; ▪ le filtrage des flux entrants et sortants, en particulier le filtrage des sites web et des flux de communication, dans le cadre de la protection de l'élève mineur ; ▪ que l'accès aux différents réseaux, filaire ou sans fil, en particulier internet, est réservé aux seules machines autorisées (parc de l'établissement et terminaux personnels enregistrés).	E	E
IN.SEC.2	Sécurité réseau	Un accès performant au réseau DOIT être une priorité dans tous les plans d'équipement des établissements/écoles. Les capacités du raccordement à internet, des point d'accès Wi-Fi, des équipements de réseau et de sécurité, et du câblage DOIVENT donc être définis en cohérence pour assurer la meilleure performance.	E	E
IN.SEC.3	Politique de sécurité	La sécurité est l'affaire de tous et repose en grande partie sur la bonne compréhension des responsabilités de chacun et donc sur la sensibilisation des acteurs (personnels, élèves, parents, collectivités territoriales, prestataires). Les principes et les règles DEVRAIENT être décrits aux différents niveaux que constituent la politique de sécurité de l'établissement ou de l'école(ex : distribution et réinitialisation des mots de passe), la charte utilisateur (ex : la non communication de ses moyens d'authentification à des tiers), le règlement intérieur (ex : entrée/sortie des équipements dans l'établissement/école), les conditions générales d'utilisation des équipements (ex : règles de sauvegarde des données situées sur les postes de travail) et/ou dans les contrats de services entre les partenaires (ex : règles d'infogérance).	R	R

APPEL COMMENTAIRE

IN.SEC.4	Filtrage	Il est indispensable de distinguer le filtrage des flux (niveaux 2 à 4 du modèle OSI), du filtrage de contenu (web, SMTP, etc.) destiné notamment à assurer la protection des mineurs et le respect des valeurs du service public de l'éducation (neutralité, etc.). Toutes les méthodes de filtrage PEUVENT être combinées (listes, analyse de contenu…) ; le service ne saurait reposer uniquement sur des listes d'autorisation, sauf contextes particuliers (très jeunes enfants ? épreuves d'examen ?).	F	F
IN.SEC.5	Filtrage	Les contextes particuliers (très jeunes enfants ? épreuves d'examen ?) et les règles applicables DOIVENT être définis par les équipes pédagogiques, hormis le filtrage des contenus manifestement illicites qui est défini au niveau national.	E	E
IN.SEC.6	Filtrage	Le service DEVRAIT proposer un mécanisme de délégation au plus près de l'acte pédagogique.	R	R
IN.SEC.7	Filtrage	Les règles de filtrage définis dans les équipements de sécurité, en particulier pour ce qui concerne la protection des mineurs, DOIVENT être sous la responsabilité de l'Education Nationale.	E	E
IN.SEC.8	Filtrage	Le service DOIT pouvoir utiliser les listes de restrictions et d'autorisations actuellement collectées et maintenues par l'université de Toulouse 1.	E	E
IN.SEC.9	Filtrage	Le service DOIT permettre l'ajout ou le retrait de règles de filtrage par les personnes autorisées de l'établissement ou de l'école.	E	E
IN.SEC.10	Filtrage	Le service DEVRAIT être capable de prendre en compte le groupe classe ou le groupe discipline, et d'une façon plus générale tout groupe pédagogique.	R	R
IN.SEC.11	Chaîne d'alerte	Une chaîne d'alerte et de responsabilités DOIT être mise en place aux niveaux local et académique pour qualifier, investiguer, traiter les incidents. Chacun a un devoir d'alerte, la détection des incidents DOIT donc être l'affaire de tous.	E	E
IN.SEC.12	Tous les services	Le service DEVRAIT permettre une administration et une exploitation de la sécurité des services (à ne pas confondre avec la gestion des règles de filtrage) centralisées.	R	R

APPEL D'OFFRE

3.2.5 Service de diffusion d'information

Service de diffusion d'information – voir le service Affichage d'informations du SDET

Ce service a pour objet de permettre la diffusion de messages (horaires, absences, menus, actualités…) sur des écrans installés dans des espaces publics ou communs de l'établissement ou de l'école (hall d'accueil, circulations, salle des professeurs…).

Impacts sur les infrastructures

Le service de diffusion fournit les infrastructures matérielles et logicielles nécessaires pour saisir, modifier, diffuser, supprimer des messages sur des écrans installés dans des espaces publics ou communs.

Le service PEUT diffuser le même contenu sur tous les écrans, sur plusieurs écrans ou diffuser un contenu différent selon les écrans. Le service PEUT proposer du multifenêtrage (plusieurs flux de contenus sur le même écran).

Le service PEUT proposer la programmation de la diffusion à des horaires prédéfinis. Il DEVRAIT être possible d'interrompre la diffusion en cours pour la diffusion de message à caractère d'urgence, sans perte du contenu initial.

Les contenus PEUVENT provenir du service de publication et le service DEVRAIT faciliter cette interopérabilité. (voir **service de publication <UT.PUB>)**

Connectique : Ces équipements DEVRAIENT utiliser les mêmes infrastructures matérielles réseau (câblage, actifs de réseau…) que les autres équipements (serveurs de fichiers, etc.) de l'établissement/école.

Accès : L'accès DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école.

Sauvegarde : Les contenus diffusés DEVRAIENT être sauvegardés, horodatés et archivés. (voir **service sauvegarde <CQ.SVG>)**

Impacts sur l'organisation

Les droits d'accès au service DOIVENT être attribués par le chef d'établissement/directeur d'école en tant que responsable de la publication.

Impacts sur la sécurité des SI

Le service ne DOIT être accessible que depuis des postes localisés dans la zone « administrative » et PEUT être protégé par authentification forte.

Toute diffusion de message DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux <CQ.JAL>)**

Aspects juridiques

Articles à consulter :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/liberte-d-expression-et-ses-limites.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/image-et-video.html

Interaction avec d'autres services

☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
IN.DIF.1	Accès	L'accès DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école.	E	E
IN.DIF.2	Accès	L'accès aux outils d'édition et de diffusion PEUT être soumis à authentification forte.	F	F
IN.DIF.3	Accès	Les droits d'accès au service DOIVENT être attribués par le chef d'établissement/directeur d'école en tant que responsable de la publication.	E	E
IN.DIF.4	Diffusion	Le service PEUT diffuser le même contenu sur tous les écrans, sur plusieurs écrans ou diffuser un contenu différent selon les écrans.	F	F
IN.DIF.5	Diffusion	Le service PEUT proposer du multifenêtrage (plusieurs flux de contenus sur le même écran).	F	F
IN.DIF.6	Diffusion	Le service PEUT proposer la programmation de la diffusion à des horaires prédéfinis	F	F
IN.DIF.7	Diffusion	Il DEVRAIT être possible d'interrompre la diffusion en cours pour la diffusion de message à caractère d'urgence, sans perte du contenu initial.	R	R
IN.DIF.8	Contenus	Les contenus PEUVENT provenir du service de publication et le service DEVRAIT faciliter cette interopérabilité	F	F
IN.DIF.9	Connectique	Le service DEVRAIT utiliser les mêmes infrastructures matérielles réseau (câblage, actifs de réseau…) que les autres équipements (serveurs de fichiers, etc.) de l'établissement/école.	R	R

IN.DIF.10	Sauvegarde/Archivage	Les contenus diffusés DEVRAIENT être sauvegardés, horodatés et archivés.	R	R
IN.DIF.11	Traçabilité	Toute diffusion de message DOIT être tracée, identifiée et horodatée.	E	E

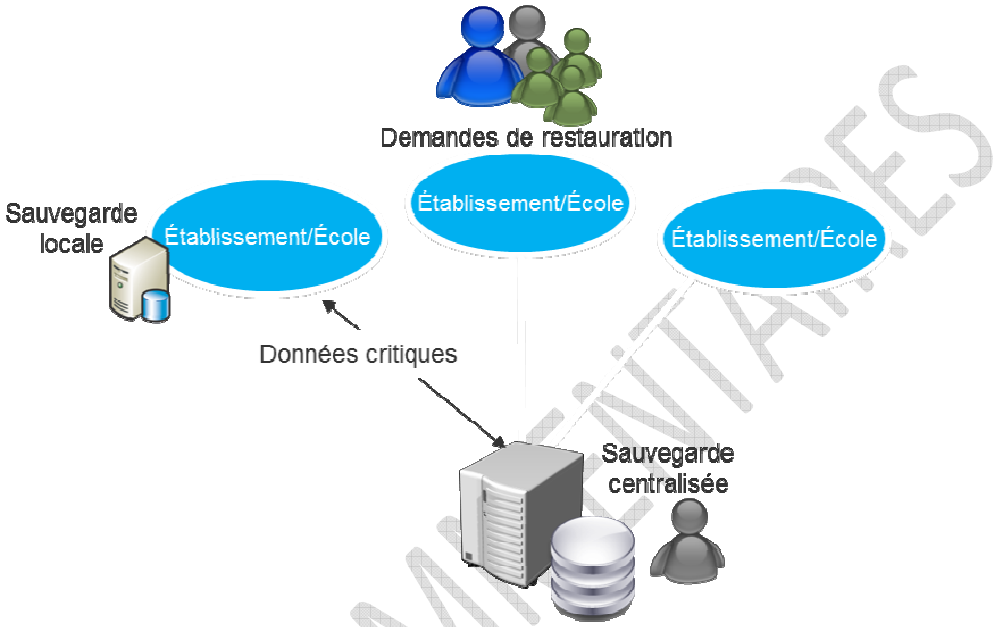
APPEL À COMMENTAIRES

3.3 Services de maintien en condition opérationnelle

3.3.1 Service de sauvegarde

Service de sauvegarde

Garantir la qualité de service passe par la préservation des données et la capacité de restaurer sur demande ces données.



Le service de sauvegarde offre les mécanismes et les procédures (fréquences, volumes, supports, lieux de stockage…) permettant de sauvegarder et de restaurer les données des utilisateurs et les données techniques sensibles.

Impacts sur les infrastructures

Les solutions de sauvegarde centralisée DEVRAIENT être mises en œuvre chaque fois que les usages et les débits le permettent.

Le service de sauvegarde DEVRAIT permettre de conserver/restaurer plusieurs versions de données sauvegardées.

Si des données administratives sont stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; Elles PEUVENT être chiffrées (chiffrement de masse ?) et DOIVENT être sauvegardées.

Certaines données font l'objet d'un cadre juridique précis quant à leur durée et conditions de rétention (journaux d'accès à internet, données comptables, données de vie scolaire, données de santé, examens et concours…). La capacité du service doit permettre de répondre aux durées légales de conservation de ces données. (voir **service de gestion des journaux <CQ.JAL>)**

Voir les instructions de tri et de conservation des archives concernant l'Education Nationale. ftp://trf.education.gouv.fr/pub/edutel/bo/2005/24/tableaux_encart24.pdf

*Pour la sauvegarde des données stockées sur les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur l'organisation

Le service de sauvegarde DOIT permettre de planifier les sauvegardes selon une politique qui définit :

- un échéancier (fréquence et calendrier),
- les critères de sélection des données à sauvegarder (arborescences, noms, extensions, dates, versions…),
- les types de sauvegardes (incrémentale, différentielle, sélective, complète).

Les procédures et mécanismes de restauration de données sauvegardées doivent être testés régulièrement. Le rythme de ces

APPEL A COMMENTAIRES

tests DEVRAIT figurer dans les clauses contractuelles ou les CGU du service.

Les utilisateurs DOIVENT être informés (charte d'établissement/école) de la durée de conservation de leurs données et de la procédure de restauration.

Le service de sauvegarde PEUT permettre l'extraction des supports de sauvegarde de telle sorte qu'ils soient stockés dans un site distant du site de production du support.

L'utilisateur doit être informé du fait que le choix du lieu de stockage de ses données a des impacts sur la sauvegarde de ses données. Cette information DOIT figurer dans la charte et/ou dans les CGU du service.

Par exemple :

- dans l'ENT ou sur les serveurs de l'établissement – données sauvegardées par le service;
- sur le disque du poste de travail – selon politique de sauvegarde de l'établissement/école,
- ailleurs (clés USB, disques externes, dans le cloud…) – données sauvegardées par l'utilisateur.

Les administrateurs techniques des sauvegardes ne DOIVENT en aucun cas accéder au contenu des sauvegardes (sauf accord de l'utilisateur ou sur demande d'une autorité judiciaire).

Impacts sur la sécurité des SI

Le service de sauvegarde est essentiel pour garantir l'intégrité et la disponibilité des données et peut avoir des conséquences sur la confidentialité.

Ces trois critères sont à considérer ensemble. Par exemple, transférer des données de l'environnement professionnel vers l'environnement grand public peut répondre au critère de disponibilité mais porter gravement atteinte à la confidentialité.

Le choix du lieu de stockage de ses données par l'utilisateur est donc l'un des facteurs de risques majeurs pour leur sauvegarde. Une sensibilisation particulière DOIT donc être programmée sur ce sujet.

Les flux des données à sauvegarder/restaurer DOIVENT être sécurisés (confidentialité et intégrité).

Aspects juridiques

Articles à consulter :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/donnees-personnelles-et-obligation-de-securite.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPELS COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
CQ.SVG.1	Sauvegarde / Restauration	Le service de sauvegarde DOIT offrir les mécanismes et les procédures (fréquences, volumes, supports, lieux de stockage…) permettant de sauvegarder et de restaurer les données des utilisateurs et les données techniques sensibles.	E	E
CQ.SVG.2	Planification	Le service de sauvegarde DOIT permettre de planifier les sauvegardes selon une politique qui définit : • un échéancier (fréquence et calendrier), • les critères de sélection des données à sauvegarder (arborescences, noms, extensions, dates, versions…), • les types de sauvegardes (incrémentale, différentielle, sélective, complète).	E	E
CQ.SVG.3	Historisation	Le service de sauvegarde DEVRAIT permettre de conserver/restaurer plusieurs versions de données sauvegardées.	R	R
CQ.SVG.4	Supports	Le service de sauvegarde PEUT permettre l'extraction des supports de sauvegarde de telle sorte qu'ils soient stockés dans un site distant du site de production du support.	F	F
CQ.SVG.5	Administration technique	Les solutions de sauvegarde centralisée DEVRAIENT être mises en œuvre chaque fois que les	R	R

		usages et les débits le permettent.		
CQ.SVG.6	Sauvegarde des données locales	Si des données administratives sont stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; Elles PEUVENT être chiffrées (chiffrement de masse ?) et DOIVENT être sauvegardées.	E	E
CQ.SVG.7	Restauration	Les procédures et mécanismes de restauration de données sauvegardées doivent être testés régulièrement. Le rythme de ces tests DEVRAIT figurer dans les clauses contractuelles ou les CGU du service.	E	E
CQ.SVG.8	Formation/Sensibilisation	Les utilisateurs DOIVENT être informés (charte d'établissement/école) de la durée de conservation de leurs données et de la procédure de restauration.	E	E
CQ.SVG.9	Formation/Sensibilisation	L'utilisateur doit être informé du fait que le choix du lieu de stockage de ses données a des impacts sur la sauvegarde de ses données. Cette information DOIT figurer dans la charte et/ou dans les CGU du service.	E	E
CQ.SVG.10	Charte administrateur technique	Les administrateurs techniques des sauvegardes ne DOIVENT en aucun cas accéder au contenu des sauvegardes (sauf accord de l'utilisateur ou sur demande d'une autorité judiciaire).	E	E
CQ.SVG.11	Transferts	Les flux des données à sauvegarder/restaurer DOIVENT être sécurisés (confidentialité et intégrité).	E	E
CQ.SVG.12	Traçabilité	Chaque sauvegarde/restauration DOIT être tracée, identifiée et horodatée.	E	E

APPEL A COMMENTAIRES

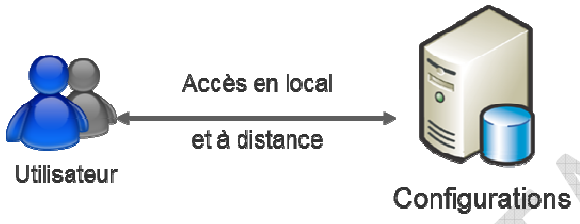
3.3.2 Service de régénération et de configuration de stations

service de régénération et de configuration de stations

En établissement/école, les postes de travail ne sont généralement pas dédiés à un seul utilisateur ou à une seule catégorie d'utilisateurs.

La mise en place d'un service de régénération et de configuration de stations garantit à l'utilisateur qu'il retrouvera un poste fonctionnel ainsi qu'un environnement de travail adapté à son usage.

Le service PEUT permettre également de choisir, lors du démarrage (boot) de la station, la configuration de la station (par exemple, dans le cas du partage de la station entre différents types d'enseignement).



Impacts sur les infrastructures

Le service offre les mécanismes et les procédures permettant de régénérer (automatiquement ou selon nécessité) la configuration d'une station de travail pour un utilisateur ou un groupe d'utilisateurs.

Le service DEVRAIT permettre de sauvegarder différentes configurations d'utilisation d'une station de travail (ergonomie, configuration système, bureau…).

La régénération de la configuration DEVRAIT être activable en local et à distance.

Une fois lancée, la régénération de la configuration DOIT être un processus automatisé.

*Pour la régénération et la configuration des terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur l'organisation

Les règles d'usage du service et en particulier les droits d'accès à la reconfiguration du poste sont définies par les équipes pédagogiques et DOIVENT être décrites dans les CGU du service.

Les utilisateurs doivent être sensibilisés au processus de partage des postes de travail et formés au mécanisme de régénération de configuration et à ses impacts (performance réseau).

Ils doivent être informés qu'un usage excessif de ce service peut avoir des conséquences sur les performances générales du réseau. Cette information DOIT figurer dans la charte de l'établissement/école ou dans les CGU du service.

Impacts sur la sécurité des SI

Le service de reconfiguration des configurations est un service essentiel pour garantir la disponibilité des postes de travail.

Ce service est souvent utilisé par les infogérants (dont les prestataires). Les règles d'accès et d'usage au service DOIVENT donc être précisées dans les CGU du service.

Aspects juridiques

Interaction avec d'autres services

☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL A COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
CQ.REG.1	Fonctionnalité	Le service DEVRAIT permettre de sauvegarder différentes configurations d'utilisation d'une station de travail (ergonomie, configuration système, bureau…).	R	R
CQ.REG.2	Démarrage	Le service PEUT permettre de choisir, lors du démarrage (boot) de la station, la configuration de la station (par exemple, dans le cas du partage de la station entre différents types d'enseignement).	F	F
CQ.REG.3	Mise à jour	Une mise à jour régulière des images DEVRAIT être opérée, notamment pour intégrer les mises à jour de sécurité des systèmes d'exploitation et des applications du poste de travail ainsi que la mise à jour des pilotes des matériels pour périphériques adaptés pour les élèves en situation de handicap.	R	R
CQ.REG.4	Activation	La régénération de la configuration DEVRAIT être activable en local et à distance.	R	R
CQ.REG.5	Automatisation	Une fois lancée, la régénération de la configuration DOIT être un processus automatisé.	E	E
CQ.REG.6	Architecture	Le service PEUT, pour faciliter la gestion centralisée (stockage des configurations), être réparti entre une partie cliente et une partie serveur.	F	F
CQ.REG.7	Accès	Les règles d'usage du service et en particulier les droits d'accès à la reconfiguration du poste sont définies par les équipes pédagogiques et DOIVENT être décrites dans les CGU du service.	E	E
CQ.REG.8	Formation/Sensibilisation	Ils doivent être informés qu'un usage excessif de ce service peut avoir des conséquences sur les performances générales du réseau. Cette information DOIT figurer dans la charte de l'établissement/école	E	E

		ou dans les CGU du service.		
CQ.REG.9	CGU	Ce service est souvent utilisé par les infogérants (dont les prestataires). Les règles d'accès et d'usage au service DOIVENT donc être précisées dans les CGU du service.	E	E

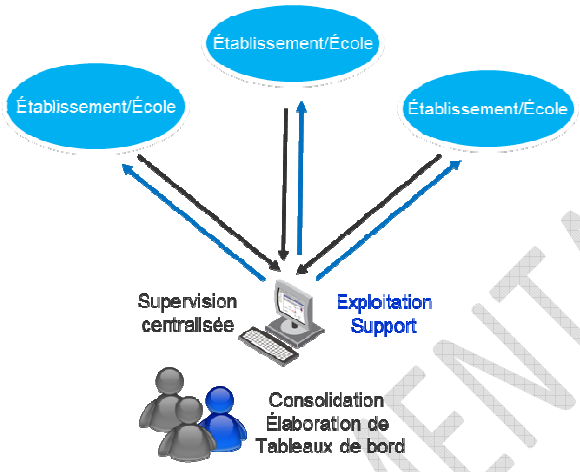
APPEL À COMMENTAIRES

3.3.3 Service de supervision et d'exploitation de l'infrastructure

Service de supervision et d'exploitation de l'infrastructure

Le service répond à deux catégories de besoins :

- Garantir la qualité du service rendu par la mise en place d'une organisation, de procédures et d'outils de supervision et d'exploitation des infrastructures en établissement/école,
- Obtenir des statistiques sur l'utilisation des services d'infrastructure.



Impacts sur les infrastructures

Collecte des données : Dans le but de faciliter la collecte, la consolidation et l'exploitation des données de supervision, le service fournit un mécanisme de remontée automatique d'informations (indicateurs, alertes…). Les données collectées peuvent concerner l'ensemble des services d'infrastructure de l'établissement ou de l'école (disponibilité des équipements et des services d'infrastructure, taux d'occupation des espaces disques, occupation de la bande passante réseau, taux d'utilisation des services…). Il est donc important d'être attentif aux impacts sur les espaces de stockage et la bande passante nécessaires.

Qualité de service :Le service doit fournir les outils permettant de mesurer la qualité des services d'infrastructure de l'établissement ou de l'école pour agir en fonction des informations remontées.

Administration : L'administration DEVRAIT pouvoir être effectuée à distance et centralisée. Un mécanisme de prise en main à distance PEUT être utilisé pour la faciliter.

Tableaux de bord : Le service DOIT fournir les outils permettant de construire des tableaux de bord à partir des données remontées des infrastructures supervisées.

Pour la supervision et l'exploitation des terminaux mobiles, se référer au ***dossier CARMO <http://CARMO>*****.**

Impacts sur l'organisation

Il existe des besoins de tableaux de bord pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes. Ces éléments peuvent provenir des informations stockées dans les journaux (voir **service de gestion des journaux<CQ.JAL>)** ou du service de gestion de parc (voir **service de gestion de parc<CQ.PAR>)**

Les administrateurs techniques doivent respecter des règles strictes pour l'accès au contenu des données collectées quand elles ont un caractère personnel ou privé (données identifiées ou identifiables). Les garanties données aux utilisateurs quant aux données les concernant DOIVENT figurer dans la charte de l'établissement/école.

APPEL À COMMENTAIRES

Ces règles DOIVENT être définies dans une charte des administrateurs techniques.

Impacts sur la sécurité des SI

L'accès aux données collectées DOIT être réservé strictement aux personnes autorisées et DEVRAIT être soumis à authentification forte. (voir **service d'authentification<IN.AUT>)**

Aspects juridiques

Pour des raisons de confidentialité, les données remontées par le service de supervision DEVRAIENT être anonymisées (par exemple via des mécanismes d'agrégation ou de calculs statistiques).

Interaction avec d'autres services

- ☐ annuaire
- ☐ poste de travail
- ☒ authentification
- ☒ sécurité et accès réseau
- ☐ diffusion d'information
- ☐ sauvegarde
- ☐ régénération de configurations
- ☐ supervision et exploitation
- ☒ gestion des journaux
- ☒ gestion de parc
- ☐ stockage / synchronisation
- ☐ messagerie électronique
- ☐ communication temps réel
- ☐ publication
- ☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
CQ.SUP.1	Prise en main à distance	L'administration DEVRAIT pouvoir être effectuée à distance et centralisée. Un mécanisme de prise en main à distance PEUT être utilisé pour la faciliter.	R	R
CQ.SUP.2	Tableaux de bord	Le service DOIT fournir les outils permettant de construire des tableaux de bord à partir des données remontées des infrastructures supervisées.	E	E
CQ.SUP.3	Tableaux de bord	Il existe des besoins de tableaux de bord pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes.	E	E
CQ.SUP.4	Administration technique	Les administrateurs techniques doivent respecter des règles strictes pour l'accès au contenu des données collectées quand elles ont un caractère personnel ou privé (données identifiées ou identifiables). Les garanties données aux utilisateurs quant aux données les concernant DOIVENT figurer dans la charte de l'établissement/école. Ces règles DOIVENT être définies dans une charte des administrateurs techniques.	E	E
CQ.SUP.5	Anonymisation	Pour des raisons de confidentialité, les données remontées DEVRAIENT être anonymisées (par exemple via des mécanismes d'agrégation ou de calculs statistiques).	R	R
CQ.SUP.6	Accès	L'accès aux données collectées DOIT être réservé strictement aux personnes autorisées ;	E	E
CQ.SUP.7	Accès	L'accès aux données collectées DEVRAIT être soumis à authentification forte.	R	R

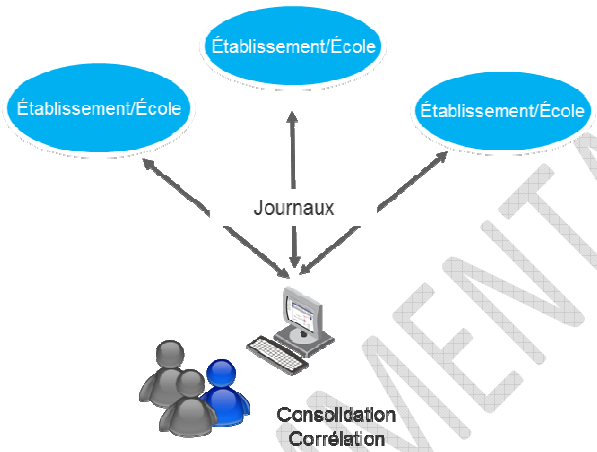
3.3.4 Service de gestion des journaux

Service de gestion des journaux

Le cadre législatif et réglementaire impose des règles en termes de traçabilité.

Les événements tracés sont enregistrés dans des journaux (ou logs).

Ces journaux sont également utiles à des fins de supervision et d'exploitation. (voir **service de supervision et d'exploitation<CQ.SUP>)**



Impacts sur les infrastructures

Les équipements générateurs de journaux DEVRAIENT respecter un format standard et commun de description d'événement.

Le service de gestion des journaux doit prévoir et décrire des procédures et mécanismes d'extraction automatique vers un format qui facilite la consolidation des journaux dans un objectif de supervision centralisée. (voir **service de supervision et d'exploitation<CQ.SUP>)**

Le service de gestion des journaux devrait offrir des mécanismes facilitant son exploitation (compression, archivage, purge,…).

Les équipements d'infrastructure peuvent être « bavards » et le stockage des journaux nécessite souvent un espace disque conséquent. La capacité du service DOIT permettre de répondre aux durées légales de conservation des données.

Le service PEUT compléter les capacités de stockage en ligne avec des mesures d'archivage sur support externe afin de répondre à cette exigence.

*Pour la gestion des journaux des terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur l'organisation

Le service de gestion des journaux constitue un service de traitement de données à caractère personnel. Les utilisateurs DOIVENT être informés (charte d'établissement/école) des durées de conservation des journaux lorsque ces derniers concernent des données à caractère personnel (journaux de l'ENT, journaux des pare-feu et des dispositifs de filtrage, journaux de connexion au Wi-Fi, journaux système par exemple).

Les besoins de consultation des journaux (quoi, par qui, à quelles fréquences, pour quel objectif …) PEUVENT être définis par le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. (voir **service de supervision et d'exploitation<CQ.SUP>)**

Les administrateurs techniques ont un accès technique aux journaux. La consultation du contenu des journaux quand ils contiennent des données à caractère personnel, sauf accord de l'utilisateur ou demande d'une autorité judiciaire doit être encadrée par des règles ; ces dernières DOIVENT être définies dans la politique de sécurité de l'établissement/école et dans une

APPEL A COMMENTAIRES

charte des administrateurs techniques.

Impacts sur la sécurité des SI

L'accès au service de gestion des journaux étant strictement réservé aux administrateurs techniques et pouvant comporter des données sensibles, il DEVRAIT être soumis à authentification forte. (voir **service d'authentification<IN.AUT>)**

En cas de centralisation de tout ou partie de la gestion des journaux, les flux entre les infrastructures de l'établissement/école et le lieu où les données sont centralisées DOIVENT être chiffrés dès lors qu'ils contiennent des données à caractère personnel.

Aspects juridiques

Dès lors que certains journaux permettent d'identifier directement ou indirectement des personnes physiques, au besoin en les croisant avec toutes données dont dispose le responsable du traitement ou toute autre personne (par exemple l'administrateur système), le système de traitement des journaux constitue un traitement de données à caractère personnel au sens de la loi du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

http://eduscol.education.fr/internet-responsable/les-tic-et-lecole/maitriser-lusage-des-reseaux/tracage-vie-privee-et-traitement-des-journaux-informatiques.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/le-droit-a-loubli.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☒ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
CQ.JAL.1	Contenu	Les équipements générateurs de journaux DEVRAIENT respecter un format standard et commun de description d'événement.	R	R
CQ.JAL.2	Capacité	Les équipements d'infrastructure peuvent être « bavards » et le stockage des journaux nécessite souvent un espace disque conséquent. La capacité du service DOIT permettre de répondre aux durées légales de conservation des données.	E	E
CQ.JAL.3	Capacité	Le service PEUT compléter les capacités de stockage en ligne avec des mesures d'archivage sur support externe afin de répondre à cette exigence.	F	F
CQ.JAL.4	Formation/Sensibilisation	Le service de gestion des journaux constitue un service de traitement de données à caractère personnel. Les utilisateurs DOIVENT être informés (charte d'établissement/école) des durées de conservation des journaux lorsque ces derniers concernent des données à caractère personnel (journaux de l'ENT, journaux des pare-feu et des dispositifs de filtrage, journaux de connexion au Wi-Fi, journaux système par exemple).	E	E
CQ.JAL.5	Consultation	Les besoins de consultation des journaux (quoi, par qui, à quelles fréquences, pour quel objectif …) PEUVENT être définis par le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école.	F	F
CQ.JAL.6	Accès	Les administrateurs techniques ont un accès technique aux journaux. La consultation du contenu des journaux quand ils contiennent des données à caractère personnel, sauf accord de l'utilisateur ou	E	E

		demande d'une autorité judiciaire doit être encadrée par des règles ; ces dernières DOIVENT être définies dans la politique de sécurité de l'établissement/école et dans une charte des administrateurs techniques.		
CQ.JAL.7	Accès	L'accès au service de gestion des journaux étant strictement réservé aux administrateurs techniques et pouvant comporter des données sensibles, il DEVRAIT être soumis à authentification forte.	E	E

APPEL À COMMENTAIRES

3.3.5 Service de gestion de parc

Service de gestion de parc

Le service répond à deux catégories de besoins :

- Garantir la maîtrise du parc informatique (matériel + services d'infrastructure) disponible en établissement/école,
- Obtenir des statistiques sur les données de ce parc et faciliter de ce fait la réponse aux enquêtes (ETIC, OPINEE…).

Le service de gestion de parc doit fournir, par établissement ou école, un dispositif permettant :

- La gestion de l'inventaire des matériels (postes de travail, serveurs, écrans, vidéo projecteurs, TNI, VNI, appareils photos, équipements réseau et de sécurité, casques audio, caméras, imprimantes, microscopes…)
- La catégorisation de ces matériels (fournisseurs, caractéristiques, vétusté, localisation, utilisation…),
- La gestion de la valeur (TCO) et des critères de remplacement et de mise au rebut,
- La réservation et le prêt de matériel,
- La gestion du cycle de vie et la planification du remplacement des équipements,
- La recherche et les statistiques,
- L'interfaçage avec le service de supervision (en particulier la gestion des incidents).

Pour la gestion du parc des terminaux mobiles, se référer au ***dossier CARMO <http://CARMO>*****.**

Impacts sur les infrastructures

Le service de gestion de parc DEVRAIT intégrer un mécanisme de découverte automatique des matériels connectés au réseau de l'établissement ou de l'école. Cela nécessite l'installation d'un agent sur les matériels de l'établissement ou de l'école, et cette recommandation devrait être prise en compte dans le choix des équipements.

Les matériels hors parc (BYOD, visiteurs, prestataires…) connectés au réseau DEVRAIENT pouvoir être détectés afin de mesurer l'impact potentiel sur les infrastructures et leur sécurité. Pour le BYOD, se référer au dossier BYOD <http://BYOD>

Impacts sur l'organisation

Il existe des besoins de tableaux de bord concernant le matériel pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes. (voir **service de supervision et d'exploitation<CQ.SUP>)**

Impacts sur la sécurité des SI

La gestion de parc constitue un apport important sur la sécurité, en particulier pour la gestion des incidents. Disposer d'un inventaire précis et à jour facilite le maintien en condition opérationnelle.

Une attention particulière doit être portée aux équipements hors parc (BYOD, visiteurs, prestataires…). On PEUT notamment leur

ARTEA COMMENTAIRES

appliquer des conditions spécifiques de raccordement au réseau de l'établissement ou de l'école.

Aspects juridiques

La gestion des déchets (dont la mise au rebut des matériels) est régie par le code de l'environnement, publié pour sa partie législative en annexe de l'Ordonnance n° 2000-914 du 18 septembre 2000 (JO du 21 septembre 2000).

La mise au rebut des matériels DOIT respecter la réglementation, en termes d'environnement et d'éventuelle cession de propriété (recyclage interne, dons (écoles, associations…), vente des domaines, sociétés privées de recyclage…).

Interaction avec d'autres services

- ☐ annuaire
- ☒ poste de travail
- ☐ authentification
- ☒ sécurité et accès réseau
- ☐ diffusion d'information
- ☐ sauvegarde
- ☐ régénération de configurations
- ☒ supervision et exploitation
- ☐ gestion des journaux
- ☐ gestion de parc
- ☐ stockage / synchronisation
- ☐ messagerie électronique
- ☐ communication temps réel
- ☐ publication
- ☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
CQ.PAR.1	Fonctionnalités principales	Le service de gestion de parc DOIT fournir, par établissement ou école, un dispositif permettant la gestion de l'inventaire des matériels (postes de travail, serveurs, écrans, vidéo projecteurs, TNI, VNI, appareils photos, équipements réseau et de sécurité, casques audio, caméras, imprimantes, microscopes…).	E	E
CQ.PAR.2	Fonctionnalités principales	L'outil de gestion de parc DEVRAIT permettre la catégorisation de ces matériels (fournisseurs, caractéristiques, vétusté, localisation, utilisation…).	R	R
CQ.PAR.3	Fonctionnalités principales	L'outil de gestion de parc DOIT permettre la recherche et les statistiques.	E	E
CQ.PAR.4	Fonctionnalités principales	L'outil de gestion de parc DEVRAIT permettre l'interfaçage avec le service de supervision (en particulier la gestion des incidents).	R	R
CQ.PAR.5	Fonctionnalités secondaires	L'outil de gestion de parc DEVRAIT permettre la gestion de la valeur (TCO) et des critères de remplacement et de mise au rebut.	R	R
CQ.PAR.6	Fonctionnalités secondaires	L'outil de gestion de parc DEVRAIT permettre la réservation de matériel.	R	R
CQ.PAR.7	Fonctionnalités secondaires	L'outil de gestion de parc PEUT permettre le prêt de matériel.	F	F
CQ.PAR.8	Découverte	Le service de gestion de parc DEVRAIT intégrer un mécanisme de découverte automatique des matériels connectés au réseau de l'établissement ou de l'école. Cela nécessite l'installation d'un agent sur les matériels de l'établissement ou de l'école, et cette recommandation devrait être prise	R	R

		en compte dans le choix des équipements.		
CQ.PAR.9	Découverte	Les matériels hors parc (BYOD, visiteurs, prestataires…) connectés au réseau DEVRAIENT pouvoir être détectés afin de mesurer l'impact potentiel sur les infrastructures et leur sécurité	R	R
CQ.PAR.10	Consultation	Il existe des besoins de tableaux de bord concernant le matériel pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes.	F	F
CQ.PAR.11	Mise au rebut	La mise au rebut des matériels DOIT respecter la réglementation, en termes environnemental et d'éventuelle cession de propriété (recyclage interne, dons (écoles, associations…), vente des domaines, sociétés privées de recyclage…) ;	E	E
CQ.PAR.12	BYOD	Une attention particulière doit être portée aux équipements hors parc (BYOD, visiteurs, prestataires…). On PEUT notamment leur appliquer des conditions spécifiques de raccordement au réseau de l'établissement ou de l'école.	F	F

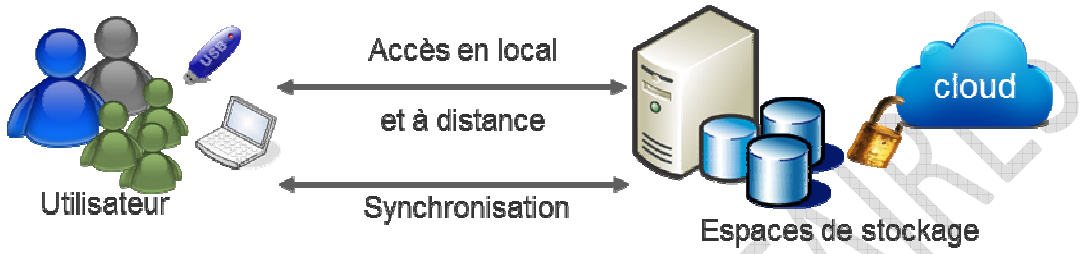
APPEL À COMMENTAIRES

3.4 Services aux utilisateurs

3.4.1 Service de stockage

Service de stockage / synchronisation – voir le service de stockage du SDET, référentiel maître sur ce sujet

Dans le cadre de leurs activités pédagogiques et administratives, les utilisateurs ont besoin d'espaces de stockage adaptés aux usages. Dans un objectif double de sécurité (sauvegarde des données) et de simplification des usages en situation de mobilité, le service de stockage DEVRAIT prévoir un mécanisme de synchronisation des données.



Le service DOIT offrir des espaces de stockage personnels et partagés à tout élève ou personnel travaillant dans l'établissement ou l'école (Le choix d'offrir un espace individuel à chaque élève du 1er degré est de la responsabilité des équipes pédagogiques). Les espaces de stockage des Services d'Infrastructures viennent compléter si besoin les espaces de stockage fournis par les ENT.

Impacts sur les infrastructures

Espaces partagés :Le service DOIT permettre de restreindre l'accès par utilisateur ou par groupe d'utilisateurs (notion d'espace de stockage partagé).

Multiplicité de supports : L'utilisation de plus en plus nomade des TIC favorise également la mise à disposition d'espaces de stockage sur des postes nomades, sur des supports amovibles (clés usb par exemple) ou sur des serveurs accessibles de partout (ex : ENT, services cloud).

Cloud : L'accès aux espaces cloud pose des questions de débit (bande passante d'accès à Internet), de confidentialité des données (localisation non maîtrisée), de réglementation (limiter les transferts de données à caractère personnel vers des pays assurant un niveau de protection suffisant).

Volumes : La capacité des espaces de stockage n'est pas illimitée. Des quotas DEVRAIENT donc être définis et il est légitime qu'ils soient surveillés en fonction des usages. Ces quotas DOIVENT tenir compte des élèves qui utilisent la LSF notamment ou beaucoup la vidéo. Ces usages nécessitent des espaces de stockage importants. Pour les élèves sourds pratiquant la LSF, la vidéo remplace l'écrit (LSF = langue première).

Stockage / Items	Dans l'ENT	Serveurs d'établissement/école	Support amovible (usb)	Cloud
Quotas	limité	limité (>ENT)	limité	illimité
Accès	Interne/externe	interne/externe via l'ENT	Interne/externe	Externe
Localisation	Etablissement/école ou académie	Etablissement/école	Non maîtrisé	Cloud public non maîtrisé
Contenus	Données établissement/école + données élèves	Données établissement/école + données classes	Non maîtrisé	Non maîtrisé

Synchronisation : Lorsque des applications ou des services enregistrent des données sur les terminaux de l'utilisateur, des mécanismes de synchronisation DEVRAIENT être proposés lorsque les débits réseau le permettent, afin de faciliter le nomadisme

DEJA COMMENTARIES

et d'augmenter le niveau de sécurité de ces données.

*Pour le stockage relatif aux données des terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur l'organisation

L'utilisateur doit être informé :

- sur les quotas de stockage des espaces qu'il utilise ;
- sur les procédures de sauvegarde/restauration mises en œuvre ;
- sur l'impact de ses choix lorsqu'il décide quelles données il stocke, où (dans l'ENT, sur les serveurs de l'établissement, dans le cloud…) et pourquoi.

Ces informations DOIVENT se retrouver dans les chartes d'établissement/écoles et/ou dans les conditions générales d'utilisation des services.

Les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais ne DOIVENT en aucun cas accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.

Les données privées de l'utilisateur DOIVENT être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…). Quand un répertoire est ainsi marqué, toute l'arborescence sous-jacente DOIT être considérée comme privée et accessible au(x) seul(s) propriétaire(s) des répertoires concernés. Ces mentions DOIVENT figurer dans la charte d'établissement / d'école.

Impacts sur la sécurité des SI

La confidentialité des données (et notamment leur caractère individuel, personnel ou privé) et la localisation des données (flux transfrontières) sont deux critères essentiels pour déterminer le lieu de stockage des données.

Les données sous la responsabilité de l'institution (espaces ENT, serveurs d'établissement/école en particulier) DOIVENT être sauvegardées régulièrement.

Aspects juridiques

Protection des mineurs : Les contenus stockés dans des espaces de stockage partagé et accessibles par un élève mineur DOIVENT respecter les exigences de protection des mineurs.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

Certaines données (journaux réglementaires par exemple) PEUVENT nécessiter la mise en place d'un mécanisme de contrôle d'intégrité (pour s'assurer qu'elles n'ont pas été modifiées).

Consulter régulièrement la rubrique « Protéger les données personnelles et la vie privée » sur http://eduscol.education.fr/internet-responsable/ressources/legamedia.html

Les fichiers structurés de données à caractère personnel DOIVENT être stockés dans des espaces qui respectent la réglementation.

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☒ régénération de configurations	☒ messagerie électronique
☐ authentification	☒ supervision et exploitation	☒ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☒ recherche documentaire

MODÈLE À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UT.STO.1	Stockage personnel	Le service DOIT offrir un espace de stockage individuel et sauvegardé à tout élève ou personnel travaillant dans l'établissement ou l'école. *Le choix d'offrir un espace individuel à chaque élève du 1er degré est de la responsabilité des équipes pédagogiques.	R*	E
UT.STO.2	Stockage partagé	Le service DOIT permettre de restreindre l'accès par utilisateur ou par groupe d'utilisateurs (notion d'espace de stockage partagé).	E	E
UT.STO.3	Gestion de quota	La capacité des espaces de stockage n'est pas illimitée. Des quotas DEVRAIENT donc être définis et il est légitime qu'ils soient surveillés en fonction des usages. Ces quotas DOIVENT tenir compte des élèves qui utilisent la LSF notamment ou beaucoup la vidéo.	R	R
UT.STO.4	Synchronisation	Dans un objectif double de sécurité (sauvegarde des données) et de simplification des usages en situation de mobilité, le service de stockage DEVRAIT prévoir un mécanisme de synchronisation des données. Synchronisation : Lorsque des applications ou des services enregistrent des données sur les terminaux de l'utilisateur, des mécanismes de synchronisation DEVRAIENT être proposés lorsque les débits réseau le permettent, afin de faciliter le nomadisme et d'augmenter le niveau de sécurité de ces données.	R	R
UT.STO.5	Données personnelles/privées	Les données privées de l'utilisateur DOIVENT être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…). Quand un répertoire est ainsi marqué, toute l'arborescence sous-jacente DOIT être considérée comme privée et accessible au(x) seul(s)	E	E

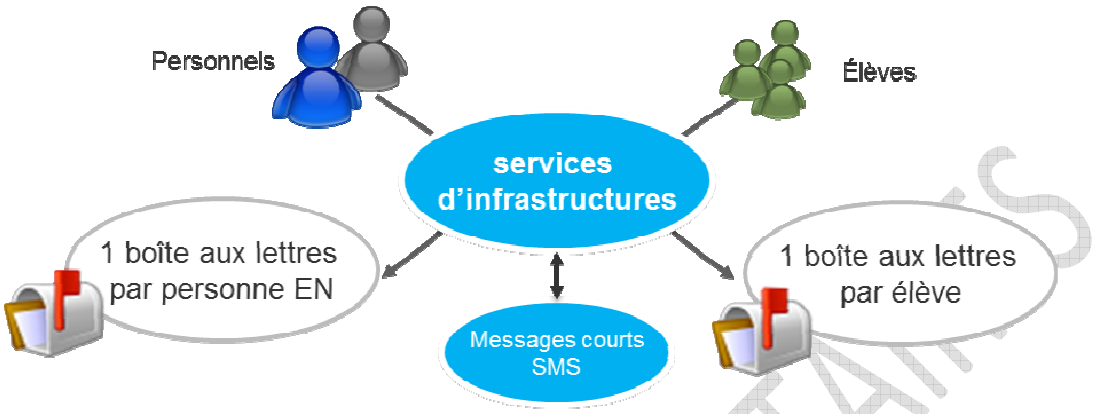
		propriétaire(s) des répertoires concernés. Ces mentions DOIVENT figurer dans la charte d'établissement / d'école.		
UT.STO.6	Formation/sensibilisation	L'utilisateur doit être informé : ▪ sur les quotas de stockage des espaces qu'il utilise ; ▪ sur les procédures de sauvegarde/restauration mises en œuvre ; ▪ sur l'impact de ses choix lorsqu'il décide quelles données il stocke, où (dans l'ENT, sur les serveurs de l'établissement, dans le cloud…) et pourquoi. Ces informations DOIVENT se retrouver dans les chartes d'établissement/écoles et/ou dans les conditions générales d'utilisation des services.	R	R
UT.STO.7	Charte administrateur technique	Les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais ne DOIVENT en aucun cas accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.	E	E
UT.STO.8	Sauvegarde	Les données sous la responsabilité de l'institution (espaces ENT, serveurs d'établissement/école en particulier) DOIVENT être sauvegardées régulièrement.	E	E
UT.STO.9	Intégrité	Certaines données (journaux réglementaires par exemple) PEUVENT nécessiter la mise en place d'un mécanisme de contrôle d'intégrité (pour s'assurer qu'elles n'ont pas été modifiées).	F	F
UT.STO.10	Protection des mineurs	Les contenus stockés dans des espaces de stockage partagé et accessibles par un élève mineur DOIVENT respecter les exigences de protection des mineurs.	E	E
UT.STO.11	Données à caractère personnel	Les fichiers structurés de données à caractère personnel DOIVENT être stockés dans des espaces qui respectent la réglementation.	E	E

APPEL A COMMENTAIRES

3.4.2 service de messagerie électronique

Service de messagerie électronique – voir le service Courrier électronique du SDET, référentiel maître sur ce sujet

Le service de messagerie électronique (courrier électronique et SMS) permet aux utilisateurs situés dans l'école, dans l'établissement, voire en dehors, d'envoyer et de recevoir des courriers électroniques et/ou des sms.



Le service de messagerie électronique est souvent impliqué dans d'autres processus comme la gestion des devoirs, la publication web, les forums… Il remplit alors des fonctions de transport, d'alerte ou de notification pour d'autres applications ou services. C'est un des outils majeurs de la continuité pédagogique.

*Pour les services de messagerie électronique disponibles sur les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur les infrastructures

Le service fournit les moyens pour accéder :

- à un service de courrier électronique :
  - accès à une boîte aux lettres par agent, fournie par l'académie ;
  - accès à une boîte aux lettres par élève ; dès que l'ENT est présent c'est lui qui la fournit.
- à un service de messages courts (sms).

Le service de messagerie électronique est accessible :

- à partir d'un logiciel client de messagerie (ex : thunderbird) lorsque le terminal fait partie du parc matériel de l'établissement/l'école;
- à partir de l'interface webmail de l'académie sur tout autre terminal disposant d'un navigateur compatible (https).

Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les courriers électroniques.

Le service de messages courts est accessible :

- à partir d'un logiciel installé sur un poste situé dans la zone « administrative »;
- à partir d'applications installées sur terminaux mobiles (voir **dossier CARMO <http://CARMO>.)**

Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les messages courts.

Impacts sur l'organisation

Courrier électronique

Les utilisateurs DOIVENT être informés des conséquences d'un stockage local des correspondances sur l'espace disque du poste de travail et sur les risques liés à la confidentialité et à la sauvegarde de ces données.

L'utilisation du service de courrier électronique par les élèves DOIT être soumise à des règles précisées dans la charte de l'établissement ou de l'école.

L'adresse de la boîte aux lettres « élèves » DOIT être distincte de celle que les élèves utilisent éventuellement à titre privé.

Les messages entre élèves sont privés.

Les messages privés DOIVENT être identifiés comme tel sur la messagerie professionnelle, par exemple en mettant « [PRIVÉ] » ou « [PERSONNEL] » en tête du sujet, voire « [MESSAGE PRIVÉ] ». Cette mention DOIT être portée dans la charte de l'établissement

APPEL À COMMENTAIRES

ou de l'école.

Dans la boîte aux lettres électronique de l'utilisateur, les messages placés dans des dossiers nommés « personnel » ou « privé » DOIVENT être considérés comme tels, quel que soit le libellé de leur objet. Cette mention DOIT être portée dans la charte de l'établissement ou de l'école.

Messages courts

Les droits d'accès au service de messages courts DOIVENT être attribués par le chef d'établissement/directeur d'école.

Impacts sur la sécurité des SI

Aucune copie automatique d'une boîte de messagerie professionnelle vers une boîte de messagerie privée ne DOIT être autorisée.

Le service de courrier électronique DOIT être couplé avec un système anti-virus et un système anti-spam.
L'accès au service de messages courts DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école et PEUT être protégé par authentification forte.

Toute diffusion de courrier électronique et de messages courts DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux <CQ.JAL>**)

Aspects juridiques

Un message électronique est un courrier privé lorsqu'il est envoyé à une ou plusieurs personnes physiques ou morales déterminées. Il est donc couvert par les dispositions légales concernant les correspondances privées.

L'usage privé des moyens mis à disposition dans le cadre professionnel DOIT demeurer proportionné au regard de la finalité première de ces moyens et des besoins prioritaires de la communauté scolaire.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/correspondance-privee-et-monde-numerique.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/forum.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☒ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL A COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UT.MSG.1	Courrier électronique	Le service de messagerie électronique est accessible : ▪ à partir d'un logiciel client de messagerie (ex : thunderbird) lorsque le terminal fait partie du parc matériel de l'établissement/l'école; ▪ à partir de l'interface webmail de l'académie sur tout autre terminal disposant d'un navigateur compatible (https). Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les courriers électroniques.	E	E
UT.MSG.2	Courrier électronique	L'utilisation du service de courrier électronique par les élèves DOIT être soumise à des règles précisées dans la charte de l'établissement ou de l'école.	E	E
UT.MSG.3	Courrier électronique	L'adresse de la boîte aux lettres « élèves » DOIT être distincte de celle que les élèves utilisent éventuellement à titre privé.	E	E
UT.MSG.4	Courrier électronique	Le service de courrier électronique DOIT être couplé avec un système anti-virus et un système anti-spam.	E	E
UT.MSG.5	Courrier électronique	Les utilisateurs DOIVENT être informés des conséquences d'un stockage local des correspondances sur l'espace disque du poste de travail et sur les risques liés à la confidentialité et à la sauvegarde de ces données.	E	E

APPLICATION COMMENTAIRE

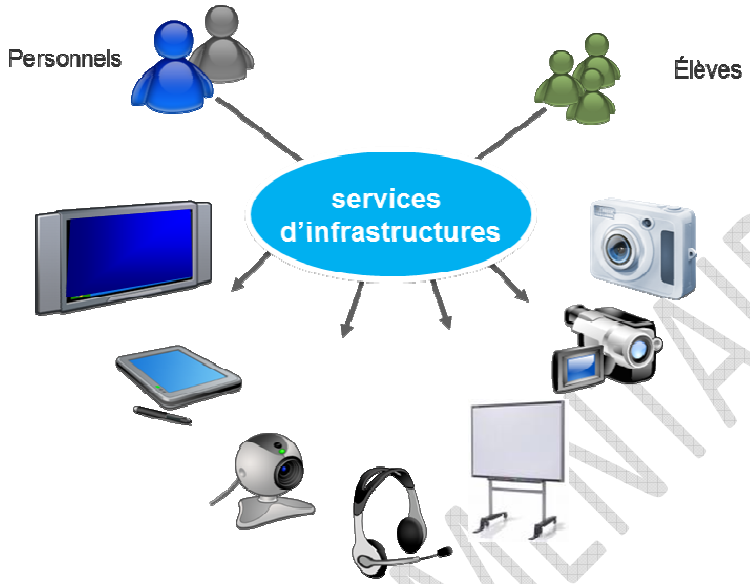
UT.MSG.6	Courrier électronique	Dans la messagerie professionnelle, les messages privés DOIVENT être identifiés comme tel sur la messagerie professionnelle, par exemple en mettant « [PRIVÉ] » ou « [PERSONNEL] » en tête du sujet, voire « [MESSAGE PRIVÉ] ».	E	E
UT.MSG.7	Courrier électronique	S'ils sont archivés sur le poste professionnel, les messages privés DOIVENT l'être dans des dossiers identifiés par leur nom ; par exemple « personnel » ou « privé ».	E	E
UT.MSG.8	Courrier électronique	Aucune copie automatique d'une boîte de messagerie professionnelle (messagerie ENT ou messagerie académique) vers une boîte de messagerie privée ne DOIT être autorisée.	E	E
UT.MSG.9	Messages courts (sms)	Le service de messages courts est accessible : ▪ à partir d'un logiciel installé sur un poste situé dans la zone « administrative »; ▪ à partir d'applications installées sur terminaux mobiles Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les messages courts.	E	E
UT.MSG.10	Messages courts (sms)	Les droits d'accès au service de messages courts DOIVENT être attribués par le chef d'établissement/directeur d'école.	E	E
UT.MSG.11	Messages courts (sms)	L'accès au service de messages courts DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école et PEUT être protégé par authentification forte.	E	E
UT.MSG.12	Vie privée résiduelle	L'usage privé des moyens mis à disposition dans le cadre professionnel DOIT demeurer proportionné au regard de la finalité première de ces moyens et des besoins prioritaires de la communauté scolaire.	E	E
UT.MSG.13	Traçabilité	Toute diffusion de courrier électronique et de messages courts DOIT être tracée, identifiée et horodatée.	E	E

APPEL A COMMENTAIRES

3.4.3 Service de communication temps réel

Service de communication temps réel – voir les services Messagerie instantanée et Conférence audio/vidéo du SDET, référentiel maître sur ce sujet

Le service de communication temps réel couvre les services qui permettent la mise en relation directe et instantanée entre plusieurs personnes.



Les Services d'Infrastructures fournissent les moyens d'accéder à des services rendus actuellement par des technologies de type tchat, téléphonie sur IP, web-conférence, visioconférence …

Ces services PEUVENT être fournis par l'ENT.

Ces services sont parfois « impliqués » dans d'autres services comme la publication web, les forums…

*Pour les services de communication temps réel disponibles sur les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur les infrastructures

Les types de services de communication temps réel utilisables en établissement ou école sont fortement dépendants de la qualité et des débits réseau disponibles.

	<200 élèves	200 à 700 élèves	700 à 1000 élèves	> 1000 élèves
Tchat	Impact faible	Impact faible	Impact faible	Impact faible
Web-conférence	Impact faible	Impact faible	Impact moyen	Impact moyen
Visioconférence	Impact fort	Impact fort	Impact fort	Impact fort

Impacts sur l'organisation

Communication interpersonnelle

Certains de ces services sont utilisés dans le cadre de communication interpersonnelle (tchat, téléphonie sur IP, web-conférence). L'accès à ces services est parfois associé à l'adresse de messagerie de l'utilisateur. Dans ces cas, seules les adresses fournies par l'institution DOIVENT être utilisées et les règles décrites dans le service de messagerie électronique dans les sections « impacts sur l'organisation », « impacts sur la sécurité des SI » et « aspects juridiques » DOIVENT s'appliquer.(voir **service de messagerie électronique<UT.MSG>)**

Impacts sur la sécurité des SI

Voir remarque sur la communication interpersonnelle.

PEL COMMENTAIRES

Aspects juridiques

Voir remarque sur la communication interpersonnelle.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/correspondance-privee-et-monde-numerique.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/espace-dexpression-collective.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/chat.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☒ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

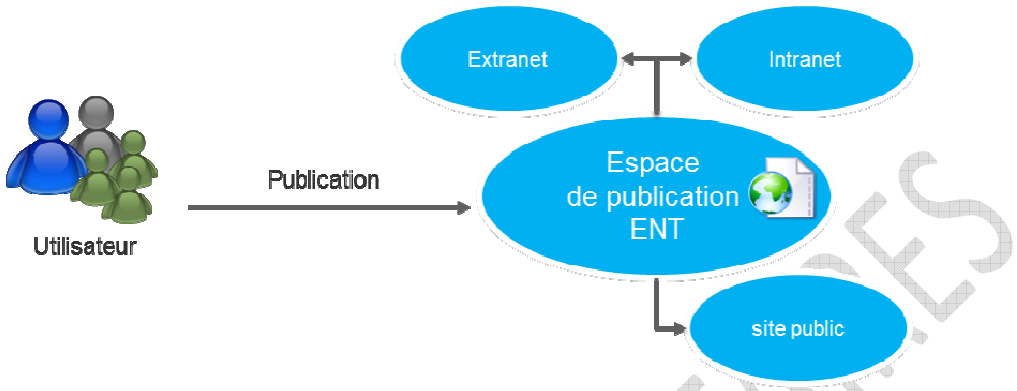
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UT.CTR.1	Fonctionnalités	Les services de communication temps réel PEUVENT être fournis par l'ENT	F	F
UT.CTR.2	Accès	Certains de ces services sont utilisés dans le cadre de communication interpersonnelle (tchat, téléphonie sur IP, web-conférence). L'accès à ces services est parfois associé à l'adresse de messagerie de l'utilisateur. Dans ces cas, seules les adresses fournies par l'institution DOIVENT être utilisées et les règles décrites dans le service de messagerie électronique dans les sections « impacts sur l'organisation », « impacts sur la sécurité des SI » et « aspects juridiques » DOIVENT s'appliquer.	E	E

APPEL À COMMENTAIRES

3.4.4 service de publication

Service de publication – voir les services Création de contenus et Publication du SDET, référentiel maître sur ce sujet

Les établissements et les écoles s'ouvrent vers l'extérieur et publient de plus en plus d'informations en ligne.



Le service offre les mécanismes et les procédures permettant de mettre à disposition des utilisateurs des outils de publication sur intranet et sur internet.

Ce service inclut les outils d'édition et de publication de contenus. Ces contenus peuvent être statiques ou dynamiques, intégrer des éléments multimédia (sons, images fixes, vidéo).

Ce service DEVRAIT être fourni par l'ENT.

Impacts sur les infrastructures

Les contenus PEUVENT être publiés en local via le service de diffusion d'information. (voir **service de diffusion <IN_DIF>**)

Les contenus PEUVENT être publiés sur internet, intranet, extranet.

Impacts sur l'organisation

Le chef d'établissement/le directeur d'école est la personne responsable des contenus édités et publiés par le personnel/les élèves de l'établissement/école.

Les droits d'accès au service (en particulier la fonction de publication sur le site public) DOIVENT être attribués sous la responsabilité du chef d'établissement/directeur d'école.

Les règles d'usage du service DEVRAIENT être décrites dans ses conditions d'utilisation.

Le service de publication DEVRAIT permettre la mise en place d'un système de contrôle et de modération.

Impacts sur la sécurité des SI

L'accès à la fonctionnalité de publication DOIT être soumise à authentification et réservé aux personnes explicitement autorisées.

Les contenus ne sont pas toujours stockés sur des espaces pris en charge par le service de sauvegarde de l'établissement ou de l'école. Les conditions de sauvegarde et de restauration des contenus DOIVENT être précisées dans les CGU du service de publication.

Aspects juridiques

La responsabilité des auteurs, des modérateurs et de l'éditeur des contenus est engagée dans tous les cas prévus par la loi (injure, diffamation, atteinte à la vie privée, etc.). Consulter les articles :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/responsabilite-sur-le-web.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/publication-en-ligne-des-eleves.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/blogue-ou-blog-information-prevention-sanction.html

APPEL A COMMENTAIRES

Interaction avec d'autres services

☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

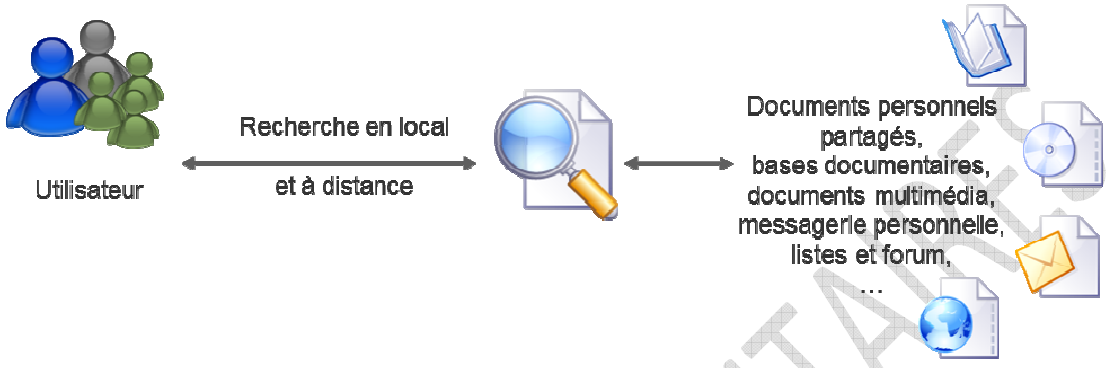
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UT.PUB.1	Fonctionnalités	Ce service DEVRAIT être fourni par l'ENT.	R	R
UT.PUB.2	Modération	Le service de publication DEVRAIT permettre la mise en place d'un système de contrôle et de modération.	R	R
UT.PUB.3	Publication	Les contenus PEUVENT être publiés en local via le service de diffusion d'information.	F	F
UT.PUB.4	Publication	Les contenus PEUVENT être publiés sur internet.	F	F
UT.PUB.5	Sauvegarde	Les contenus ne sont pas toujours stockés sur des espaces pris en charge par le service de sauvegarde de l'établissement ou de l'école. Les conditions de sauvegarde et de restauration des contenus DOIVENT être précisées dans les CGU du service de publication.	E	E
UT.PUB.6	Accès	Les droits d'accès au service (en particulier la fonction de publication de site public) DOIVENT être attribués sous la responsabilité du chef d'établissement/directeur d'école.	E	E
UT.PUB.7	Charte	Les règles d'usage du service DEVRAIENT être décrites dans la charte de l'établissement/école.	E	E
UT.PUB.8	Authentification	L'accès à la fonctionnalité de publication DOIT être soumise à authentification et réservé aux personnes explicitement autorisées.	E	E

3.4.5 service de recherche documentaire

Service de recherche documentaire – voir le service de recherche du SDET, référentiel maître sur ce sujet

Dans le but de faciliter l'accès des utilisateurs aux informations, ce service met à disposition un outil de recherche documentaire multi-critères s'appuyant sur des outils d'indexation.

La recherche peut porter sur des données structurées ou non (fichiers, fichiers audio/vidéo, pages Web, courriels et pièces attachées, forums, etc.).



Ce service DEVRAIT être accessible de partout.

*Pour la recherche sur les données stockées sur les terminaux mobiles, se référer au **dossier CARMO <http://CARMO>**.*

Impacts sur les infrastructures

L'utilisateur DOIT pouvoir effectuer des recherches sur l'ensemble des données accessibles depuis le poste de travail professionnel (données stockées sur le poste, données de l'ENT, données stockées sur des serveurs académiques, bases documentaires, etc.).

Le service DEVRAIT permettre des recherches unifiées (notion de méta moteur) sur les données.

Impacts sur l'organisation

Les utilisateurs DOIVENT être informés sur l'intérêt et sur les impacts (confidentialité) du stockage des données sur des espaces partagés ouverts au service d'indexation et de recherche.

Impacts sur la sécurité des SI

Le service de sécurité DOIT veiller à ce que le service de recherche ne permette pas à l'utilisateur d'accéder à des données qu'il n'est pas autorisé à consulter.

Aspects juridiques

Protection des mineurs : Lorsqu'il existe, le filtrage des résultats affichés par le service de recherche DEVRAIT s'appuyer sur les mêmes règles que le dispositif de filtrage web.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

http://www.jeunes.cnil.fr/

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

APPEL À COMMENTAIRES

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UT.REC.1	Recherche	L'utilisateur DOIT pouvoir effectuer des recherches sur l'ensemble des données accessibles depuis un poste de travail professionnel (données stockées sur le poste, données de l'ENT, données stockées sur des serveurs académiques, bases documentaires, etc.).	E	E
UT.REC.2	Méta moteur	Le service DEVRAIT également permettre des recherches unifiées (notion de méta moteur) sur les données.	R	R
UT.REC.3	Accès	Ce service DEVRAIT être accessible de partout.	R	R
UT.REC.4	Données partagées	Les utilisateurs DOIVENT être informés sur l'intérêt et sur les impacts (confidentialité) du stockage des données sur des espaces partagés ouverts au service d'indexation et de recherche.	E	E
UT.REC.5	Sécurité	Le service de sécurité DOIT veiller à ce que le service de recherche ne permette pas à l'utilisateur d'accéder à des données qu'il n'est pas autorisé à consulter.	E	E
UT.REC.6	Protection des mineurs	L'accès des mineurs aux contenus remontés par le service de recherche DEVRAIT être contrôlé et protégé.	R	R

APPLICABLE AUX MARCHÉS

4. Positionnement dans le référentiel documentaire

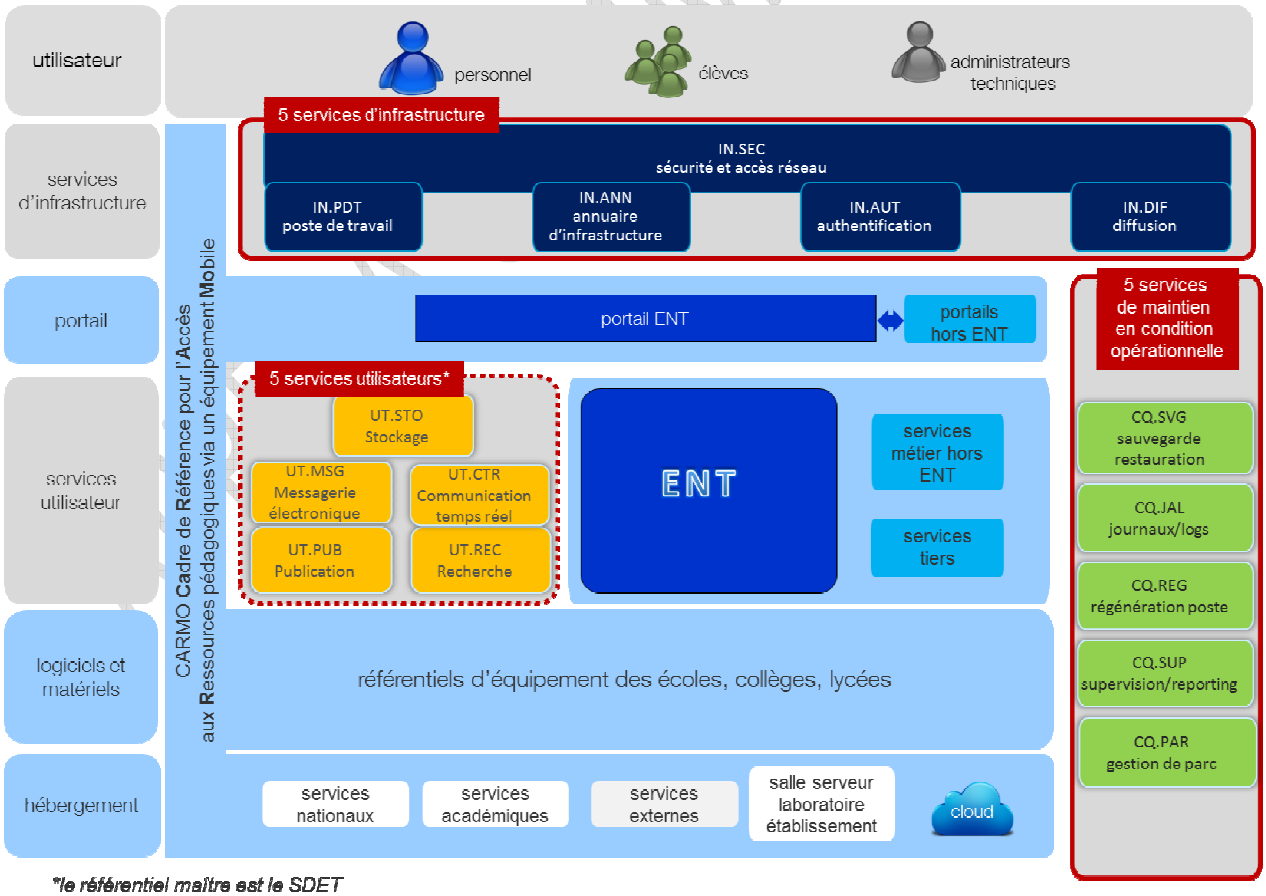
Le S3IT, Schéma Stratégique des Systèmes d'information et de Télécommunications, définit les grands axes stratégiques et fournit la feuille de route pour le déploiement des services numériques pour l'éducation.

Le S3IT, le SDSSI et le SDET couvrent 1er degré, 2d degré et supérieur.

Les Services d'Infrastructures Numériques ne couvrent que le 1er et le 2d degrés.

D'autres documents viennent compléter le référentiel :

- le SDET, schéma directeur des espaces numériques de travail, qui définit un bouquet de services à destination des utilisateurs des 1er et 2d degrés ;
- les référentiels d'équipement qui permettent d'évaluer et de projeter les besoins matériels d'une école ou d'un établissement du 2d degré ;
- le Cadre de référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile (CARMO) pour l'utilisation de terminaux mobiles de type tablettes notamment, et affectés aux élèves de façon individuelle.



"le référentiel maître est le SDET

5. Historique et principales nouveautés

Le système éducatif s'est largement engagé ces dernières années dans la voie de l'appropriation des technologies de l'information et de la communication. Des efforts importants ont été déployés, avec une implication forte des collectivités territoriales, pour développer l'équipement et la mise en réseau des établissements.

De nombreux services numériques sont aujourd'hui à la disposition des élèves, de leurs parents, des enseignants et des personnels administratifs.

Les nouveaux programmes, ont, pour la plupart, intégré l'usage des technologies de l'information et de la communication dans les objectifs et méthodes d'enseignement et d'apprentissage, tant dans l'enseignement primaire que dans les disciplines de l'enseignement secondaire. Au-delà de leur prise en compte dans les disciplines, les technologies de l'information et de la communication sont devenues une compétence de base du citoyen, dans sa vie privée et professionnelle et cette dimension est prise en compte par le système éducatif notamment avec la création au cours de l'année 2000 du Brevet informatique et internet (B2i), qui définit les compétences de base que doit acquérir tout élève dans ce domaine.

Dans ce contexte, le ministère apporte son soutien au développement des usages, par des actions d'accompagnement. Deux grandes catégories d'actions ont été engagées ces dernières années :

- des actions de mise en cohérence des services mis à la disposition des utilisateurs, notamment à travers les projets, « Schéma Directeur des Infrastructures », « espaces numériques de travail » et « espaces numériques des savoirs »,
- des actions d'accompagnement et d'assistance aux utilisateurs des TIC.

Le projet « Services internet-intranet d'établissements scolaires et d'écoles[1] » (S2i2e) mené dans le cadre du « Schéma Directeur des Infrastructures », a été lancé en 2002, dans le but de donner le maximum de cohérence aux services internet et intranet mis en place pour des besoins spécifiques des équipes administratives et pédagogiques des établissements scolaires et des écoles primaires[1]. Une note de cadrage a été réalisée, à destination des acteurs régionaux, notamment des académies en partenariat avec les collectivités territoriales, pour aider à la définition des infrastructures correspondantes.

(http://tice.education.fr/educnet/Public/services/infrastructures/S2i2e)

Depuis 2002, un effort considérable a été accompli dans les académies, en partenariat avec les collectivités territoriales. Aujourd'hui, l'ensemble des collèges et des lycées est connecté à internet, et des solutions S2i2e sont déployées dans la grande majorité des établissements. En revanche, le déploiement n'est pas généralisé à ce jour dans les écoles.

La démarche de structuration des services TIC mis à la disposition des utilisateurs, engagée notamment à travers des projets tels que les espaces numériques de travail et l'Espace Numérique des Savoirs,

[1] Maternelles et Elémentaires

APPEL À COMMENTAIRES

conduisent aujourd'hui les acteurs locaux (services académiques et collectivités territoriales) à redéfinir les collaborations en les replaçant dans une approche de partenariat global. Il s'agit, pour les partenaires, de faire évoluer leurs rôles respectifs pour permettre un développement cohérent des usages, en se répartissant les diverses fonctions à assurer.

Cette répartition doit en particulier être étudiée pour les fonctions assurées par les Services d'Infrastructures Numériques qui constituent désormais un élément stratégique des dispositifs TIC académiques. Ils conditionnent le développement des usages administratifs et pédagogiques ; ils facilitent l'accès aux ENT et à d'autres services numériques de plus haut niveau, locaux ou distants (portail, gestion de contenus…) ; ils assurent en grande partie la sécurité des systèmes d'information et la protection des mineurs ; ils conditionnent donc le développement des usages des TIC.

Le ministère a lancé en avril 2005 une étude de façon à dégager des éléments concrets permettant aux académies, en relation avec leurs partenaires des collectivités territoriales, de disposer des éléments de décisions pour définir les évolutions éventuelles de leur dispositif SIN en vue de pérenniser et d'assurer la qualité des services dans tous les établissements scolaires et écoles primaires, et en particulier :

- de disposer d'un état des lieux des solutions S2i2e déployées dans les académies, ainsi que d'une analyse des besoins dans ce domaine,
- d'analyser les axes de rationalisation et d'amélioration des services S2i2e,
- de préconiser des orientations et des évolutions.

Cette étude sur l'état des lieux et les besoins relatifs aux S2i2e a mis en exergue sept constats principaux :

> Constat n°1 : Les S2i2e, tels que définis dans la note de cadrage de 2002, sont massivement déployés ou dans une phase de déploiement massif dans les collèges et les lycées. Mis à part quelques cas particuliers remarquables, le 1er degré[2] est fortement sous-équipé.

> Constat n°2 : Les services proposés, tels que définis dans la note de cadrage, qu'ils soient basés sur des solutions libres conçues en interne ou sur des outils du marché, fonctionnent bien et rendent le service qu'on en attend.

> Constat n°3 : Nombre de solutions situées au cœur des S2i2e (pare-feux, filtrage d'url, serveurs de publication, outils de supervision…) sont conçues, développées, maintenues par l'éducation nationale qui assume le rôle d'éditeur logiciel. Ces solutions sont parfois concurrentes.

> Constat n°4 : Les besoins des utilisateurs, hormis le cas particulier des filières techniques, sont relativement basiques et bien desservis aujourd'hui par les outils mis à disposition.

> Constat n°5 : Les régions et les départements sont fortement mobilisés sur l'équipement des collèges et des lycées. Leur intervention s'effectue généralement en bonne coordination avec les équipes des rectorats. Dans les écoles, l'implication des communes est variable.

[2] Une note complémentaire sur les spécificités du 1er degré est annexée au cadre de référence.

APPEL A COMMENTAIRES

> Constat n°6 : L'organisation mise en place dans les académies pour les phases d'acquisition et d'installation d'équipement matériel et logiciel a permis de répondre aujourd'hui au besoin. Le déploiement est assuré majoritairement par l'éducation nationale.

> Constat n°7 : La tension est très forte sur les phases de maintenance, d'exploitation et de support aux utilisateurs. Le système fonctionne aujourd'hui grâce à une multitude d'actions isolées, insuffisamment cadrées et s'appuyant en partie sur de lourds investissements personnels. Ce déficit de cadre directeur sur la « maintenance en condition opérationnelle » des S2i2e, outre le fait que cela génère un mécontentement général, pose la question de la pérennité et de la qualité des services mis en place. Cette fonction est diversement assurée selon les partenariats mis en œuvre entre les différentes collectivités et les académies.

Ces constats ont permis l'élaboration et la publication en 2008 d'un cadre de référence des S2i2e.

Depuis 2008, les besoins, les usages, les technologies et les offres de service ont évolué, plus encore qu'au cours des six années de la période précédente.

Par ailleurs, le CRS2i2e s'articule avec le schéma directeur des espaces numériques de travail (SDET) qui entre en 2014 dans une nouvelle phase d'évolution et il existe des problématiques communes à ces deux référentiels.

La version 1.0 du CRS2i2e a été appréciée par ses destinataires et jugée propre à remplir sa principale fonction : constituer un outil de référence et de dialogue entre les parties concernées par la conception, la réalisation et la mise en œuvre de services intranet / internet d'établissements scolaires et d'écoles. Outre la prise en compte de nouveaux services, les axes de travail choisis pour la refonte de ce référentiel en 2013, ont été les suivants :

- Intégration des problématiques spécifiques induites par la mobilité et les terminaux personnels.
- Description plus fine des besoins fonctionnels métier concernant certains services utilisateurs.
- Intégration d'outils tels que des modèles de grilles d'analyse, de charte d'usage.

Une étude, lancée en 2014, a permis d'identifier les points forts/points faibles du référentiel de 2008. Suite à ces constats, le référentiel a été réactualisé en 2015 pour tenir compte d'évolutions de contenu (ajout/modification de service, prise en compte de la mobilité, liens vers textes réglementaires…) et de forme (navigation web dans le référentiel, recherche facilitée, actualisation simplifiée…).

APPEL À COMMENTAIRES

6. Annexes

6.1 Documents de référence

Documents de référence

Pointeur	Titre
[NCS2i2e]	Note de cadrage des S2i2e - 2007
[SDET]	Schéma directeur des espaces numériques de travail V4 - 2012
[SDSSI]	Schéma directeur de la sécurité des systèmes d'information - 2005

6.2 Glossaire

Terme	Définition
CARINE	CAdre de Référence des services d'Infrastructures Numériques d'Etablissements scolaires et d'écoles
Charte d'établissement/école	Document définissant les droits et devoirs des utilisateurs des services numériques de l'établissement/école
Charte administrateur technique	Document définissant les droits et devoirs des administrateurs techniques des services numériques de l'établissement/école
Communauté éducative	Dans chaque école, collège ou lycée, la communauté éducative rassemble les élèves et tous ceux qui, dans l'établissement scolaire ou en relation avec lui, participent à l'accomplissement de ses missions. Elle réunit les personnels des écoles et établissements, les parents d'élèves, les collectivités territoriales, les associations éducatives complémentaires de l'enseignement public ainsi que les acteurs institutionnels, économiques et sociaux, associés au service public de l'éducation.
CRS2i2e	Cadre de Référence des S2i2e
Espace individuel	Espace dont l'usage est réservé à une personne. Des droits limités sur tout ou partie de cet espace peuvent être concédés à d'autres utilisateurs que le propriétaire, soit en vertu de règles organisationnelles écrites et connues de tous, soit par le propriétaire lui-même.
Espace personnel	Espace réservé à l'usage exclusif d'une personne et dont la confidentialité est garantie. Ne préjuge pas de l'usage principalement professionnel ou privé de l'espace.
Espace privé	Espace personnel réservé à des données considérées comme privée.
ENT (Espace Numérique de Travail)	Un espace numérique de travail (ENT) désigne un ensemble intégré de services numériques choisis et mis à disposition de tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire dans un cadre de confiance. Il constitue un point d'entrée unifié permettant à l'utilisateur d'accéder, selon son profil et son niveau d'habilitation, à ses services et contenus numériques. Il offre un lieu d'échange et de collaboration entre ses usagers, et avec les autres communautés en relation avec l'école ou l'établissement.
EPLE	Etablissements Publics Locaux d'Enseignement
HTTP / HTTPS	Hyper Text Transport Protocol et sa version sécurisée basée sur SSL (Secure Socket Layer)
IA	Inspecteur d'académie
IEN	Inspecteur de l'éducation nationale

APPEL À COMMENTAIRES

Terme	Définition
LDAP (Lightweight Directory Access Protocol)	Protocole reposant sur TCP/IP permettant l'interrogation et la modification des services d'annuaire. LDAP a évolué vers une norme qui inclut un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication
MAM	Mobile Application Management
MCM	Mobile Content Management
MDM	Mobile Device Management
MxM	Couvre les acronymes MDM, MAM et MCM
Mode dégradé	Fonctionnement des services de manière partielle ou ralentie suite à un dysfonctionnement. Une organisation particulière permet de poursuivre l'exploitation tout en préparant le dépannage.
PIA	Portail Intranet Académique
POP3 / IMAP4	Protocole standard pour la récupération de mèl sur un serveur SMTP
Proxy	On parle de serveur proxy pour désigner un dispositif qui gère des accès indirects à des ressources. Ce mécanisme dit « en coupure » permet la gestion de filtres (ex : listes d'exclusion d'url) et intègre parfois des mécanismes de cache pour optimiser les performances d'accès à des données fréquemment consultées.
RACINE et RACINE-AGRIATES	Réseau d'Accueil et de Consolidation des Intranets de l'Éducation Nationale Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Etablissements Scolaires
Reverse-Proxy	Un proxy gère les sorties vers l'extérieur d'un SI. Un reverse-proxy gère les entrées vers le SI en intervenant en coupure entre les clients externes et les services internes.
RGI	Le Référentiel Général d'Interopérabilité (RGI) spécifie un ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public, pour assurer la simplicité d'intégration de nouveaux systèmes et pour faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs. L'interconnexion des systèmes, favorisée par le RGI, ne doit pas se faire au détriment de la sécurité. (http://www.modernisation.gouv.fr)
RGS	Le Référentiel Général de Sécurité (RGS) apporte des méthodologies entre autres de conception, développement et exploitation permettant de renforcer la sécurité, et spécifie l'ensemble des règles que doivent respecter les fonctions de sécurité, comme l'identification, l'authentification, la signature... Par ailleurs, il définit des niveaux de sécurité sur lesquels doivent se caler les applications et les dispositifs afin d'assurer en la matière la cohérence des systèmes amenés à interagir. (http://www.modernisation.gouv.fr)
SDET	Schéma Directeur des Espaces Numériques de Travail
SDI	Schéma Directeur des Infrastructures
SDSSI	Schéma Directeur de la Sécurité des Systèmes d'Information
S2i2e	Services intranet/internet d'établissements scolaires et d'écoles
SI (Système d'Information)	Ensemble des ressources fonctionnelles, techniques et humaines qui permet de stocker, traiter, ou transmettre l'information
SMTP (Simple Mail Transfer Protocol)	Protocole standard pour les échanges de messages
SSO (Single Sign-On)	Mécanisme permettant à un utilisateur de s'authentifier une seule fois et d'obtenir l'accès à plusieurs ressources logicielles.
TIC	Technologies de l'information et de la communication
TICE	Technologies de l'information et de la communication pour l'éducation

APPEL À COMMENTAIRES

Terme	Définition
USB (Universal Serial Bus)	Technologie permettant de brancher des périphériques sur un équipement
Visioconférence	Technologie qui permet de voir et de dialoguer avec un ou plusieurs (visioconférence multipoints) interlocuteurs.
XML (eXtensible Markup Language)	Langage informatique de balisage, dont l'objectif principal est de faciliter l'interopérabilité (échange automatisé de contenus entre systèmes d'informations hétérogènes).

APPEL À COMMENTAIRES