

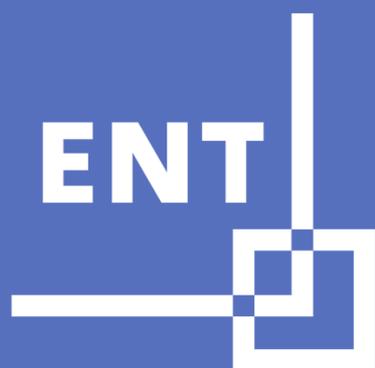


**MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS**

*Liberté
Égalité
Fraternité*

SDET

Schéma Directeur des Espaces numériques
de Travail pour l'enseignement scolaire



Espace numérique de travail

Annexe Opérationnelle
version 6.4
Juin 2021

CC BY SA 3.0 FR

Table des matières

1. Introduction	7
1.1. Organisation du SDET.....	7
1.2. Organisation de l'annexe opérationnelle.....	8
1.3. Niveaux d'exigence des recommandations formulées	8
2. Authentification–Autorisation–SSO (AAS)	10
2.1. Introduction	10
2.2. Fédération d'identités	11
2.2.1. Domaine de confiance.....	11
2.2.2. Fournisseur d'identité.....	12
2.2.3. Fournisseur de service.....	12
2.2.4. Fournisseur d'attributs.....	12
2.2.5. Service de découverte du fournisseur d'identité	12
2.2.6. Accords de fédération.....	13
2.2.7. Récapitulatif des exigences et recommandations	14
2.3. Propagation des informations d'identité entre l'ENT et les services externes au projet ENT ...	15
2.3.1. Généralités.....	15
2.3.2. Données partagées	17
2.3.3. Fonctions proposées.....	17
2.3.4. Cinématiques d'accès.....	17
2.3.5. Récapitulatif des exigences et recommandations	23
2.4. Cas des guichets et des portails de service mis en œuvre par l'Éducation nationale	23
2.4.1. Agents.....	24
2.4.2. Élèves et représentants légaux des élèves.....	24
2.4.3. Récapitulatif des exigences et des recommandations.....	26
2.5. Cas du guichet d'authentification de l'enseignement agricole.....	27
2.6. Exigences et recommandations pour l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités.....	27
2.6.1. Présentation des différentes catégories de services Tiers	28
2.6.2. Exigences et recommandations fonctionnelles.....	28
2.6.3. Conventions de service	40
2.6.4. Récapitulatif des exigences et recommandations	42
3. Méthodes d'intégration	46
3.1. Introduction	46
3.2. Interface applicative de Programmation (API).....	46
3.2.1. Présentation.....	46
3.2.2. APIisation de l'ENT	47
3.2.3. Exposition de données et des services	48
3.2.4. Versionning des API.....	48
3.2.5. Récapitulatif des exigences et recommandations	49
4. Stratégie d'exploitation	50
4.1. Introduction	50
4.2. Les prestataires et la contractualisation	50
4.2.1. Principes généraux.....	51
4.2.2. Relations entre intégrateur et mainteneur	51
4.2.3. Relations entre hébergeur/exploitant et intégrateur/éditeur/mainteneur	52
4.2.4. Propriété des matériels et logiciels.....	53
4.2.5. Qualités des prestataires extérieurs et exigences contractuelles.....	54
4.3. Les moyens de qualifier la solution ENT.....	55
4.4. Fourniture et évolutions de l'ENT.....	57
4.4.1. Fourniture initiale.....	57

4.4.2. Maintenance.....	57
4.4.3. Les étapes préalables à une mise en exploitation	60
4.4.4. Livrables.....	61
4.4.5. Tests	62
4.4.6. Définition du planning de déploiement.....	63
4.4.7. Gestion de projet et des risques en phase de maintenance et d'exploitation.....	63
4.4.8. Audits.....	63
4.4.9. Réversibilité.....	63
4.4.10. Changement de solution ENT	64
4.5. Récapitulatif des exigences et recommandations.....	67

5. Nomenclatures 74

5.1. Introduction	74
5.2. Codes des projets ENT	75
5.2.1. Codes avant la réforme territoriale.....	75
5.2.2. Codes après la réforme territoriale.....	78
5.3. Regroupement d'écoles ou d'établissements : RPI, cités scolaires	82
5.3.1. RPI (regroupements pédagogiques intercommunaux)	82
5.3.2. Cités scolaires.....	82
5.4. Nomenclatures des MEF.....	83
5.4.1. Généralités.....	83
5.4.2. Thématique de la formation	84
5.4.3. Classification de la formation par rapport à un cursus	88
5.4.4. Synthèse des informations disponibles à partir d'un MEF national.....	91
5.5. Enseignements, disciplines et niveaux des formations.....	92
5.5.1. Nomenclatures « de gestion » utilisées par le MEN.....	92
5.5.2. Correspondances BCN / ScoLOMFR	93
5.5.3. Correspondances BCN / nomenclatures de l'enseignement agricole.....	95
5.6. Informations de scolarité transmises par le SI du MEN.....	95
5.6.1. Nomenclatures académiques transmises dans le second degré par le biais de l'annuaire académique fédérateur (AAF).....	96
5.6.2. Informations transmises pour les élèves du second degré.....	97
5.6.3. Informations transmises pour les enseignants de l'Éducation nationale du second degré	99
5.7. Profils de l'accédant.....	101
5.8. Personnes en relation avec les élèves.....	102
5.8.1. Premier degré.....	102
5.8.2. Second degré	103
5.9. Récapitulatif des exigences et recommandations.....	104

6. Médiacentre 105

6.1. Introduction	105
6.2. Ressources du Médiacentre.....	105
6.3. Fonctionnalités du Médiacentre.....	106
6.4. Cas des utilisateurs multi-établissements.....	107
6.5. Récapitulatif des exigences et recommandations.....	107

7. ENT et Gestionnaire d'accès aux ressources (GAR) 109

7.1. Introduction	109
7.2. Provisionnement des données du GAR.....	110
7.3. ENT fournisseur d'identité.....	110
7.4. Liste des ressources affectées.....	110
7.5. Accès à la ressource.....	111

8. Ensemble annuaire	112
8.1. Documents de l'ensemble annuaire	112
8.2. Recommandations pour l'ensemble annuaire.....	113
9. Aspects juridiques	114
9.1. Préambule.....	114
9.2. Droit et ENT.....	114
9.2.1. Code de l'éducation	115
9.2.2. Code de la propriété intellectuelle.....	115
9.2.3. Loi relative à l'Informatique, aux fichiers et aux libertés modifiée & RGPD	116
9.2.4. Circulaires	117
9.2.5. Référentiels.....	118
9.2.6. Espace de droit	118
9.2.7. Espace de travail.....	119
9.2.8. À retenir	119
9.3. Contrats et ENT	119
9.3.1. Premier niveau : portage du projet ENT via une convention de partenariat	120
9.3.2. Deuxième niveau : sécurisation des traitements de données personnelles via une convention de responsabilité de traitement conjointe adossée à la convention de partenariat	120
9.3.3. Troisième niveau : réalisation et acquisition d'une solution ENT	121
9.3.4. Quatrième niveau : contrats avec les utilisateurs	124
9.3.5. À retenir	124
9.4. Accès et conditions d'utilisation.....	124
9.4.1. Droits des utilisateurs	125
9.4.2. Obligations des utilisateurs.....	125
9.4.3. Identification / authentification	126
9.4.4. Responsabilité.....	126
9.4.5. Obligation de protection des données personnelles	126
9.4.6. À retenir	126
9.5. Protection des données à caractère personnel.....	127
9.5.1. Principes fondamentaux applicables au traitement des données à caractère personnel	127
9.5.2. Responsable de traitement	131
9.5.3. À retenir	132
9.6. Identification / authentification	132
9.6.1. Identifiants.....	132
9.6.2. Présomption	133
9.6.3. À retenir	133
9.7. Usurpation d'identité numérique.....	134
9.7.1. À retenir	135
9.8. Espaces d'échanges et de collaboration.....	135
9.8.1. À retenir	136
9.9. Messagerie électronique et messagerie instantanée	136
9.9.1. Messagerie électronique.....	136
9.9.2. Messagerie instantanée	137
9.9.3. À retenir	137
9.10. Espace individuel.....	138
9.10.1. À retenir	138
9.11. ENT et responsabilités.....	138
9.11.1. À retenir	139
9.12. Droit des tiers.....	139
9.12.1. Propriété littéraire et artistique	140
9.12.2. Vie privée et droit à l'image.....	140
9.12.3. À retenir	141

9.13. Traçabilité.....	141
9.13.1. À retenir	142
9.14. Sécurité et confidentialité des données.....	142
9.14.1. Obligation de sécurité	143
9.14.2. Confidentialité.....	145
9.14.3. À retenir	145
9.15. Atteinte à l'ENT.....	145
9.15.1. À retenir	146
9.16. Audit et contrôle.....	146
9.16.1. À retenir	147
9.17. Suivi des accès, cookies et statistiques	147
9.17.1. À retenir	147
9.18. Conservation des données.....	148
9.18.1. Principes	148
9.18.2. Conservation du cahier de textes numérique.....	148
9.18.3. Conservation des données à caractère personnel.....	148
9.18.4. À retenir	149
9.19. Commerce électronique.....	149
9.19.1. À retenir	150
9.20. Exigences et recommandations juridiques relatives aux aspects juridiques des ENT	151

10. Grilles de conformité

153

Table des illustrations

Figure 1 : Organisation du SDET et de la documentation d'accompagnement.....	7
Figure 2 : Niveau d'exigence des recommandations.....	8
Figure 3 : Concepts clé de la fédération d'identités.....	11
Figure 4 : Propagation des informations d'identité.....	16
Figure 5 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis le portail de l'ENT	18
Figure 6 : Authentification déléguée à un fournisseur d'identité externe et accès à un fournisseur de service externe depuis le portail de l'ENT.....	19
Figure 7 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis un portail externe	20
Figure 8 : ENT fournisseur d'identité et accès à un service externe depuis le portail de l'ENT	22
Figure 9 : Cinématique fonctionnelle pour les services de catégorie 1.....	29
Figure 10 : Cinématique fonctionnelle pour les services de catégorie 2.....	30
Figure 11 : Cinématique fonctionnelle pour les services de catégorie 3	32
Figure 12 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la première connexion)	35
Figure 13 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la connexion nominale).....	36
Figure 14 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la première connexion)	38
Figure 15 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la connexion nominale).....	39
Figure 16 : Echanges entre l'ENT et les services externes de l'ENT via API.....	47
Figure 17 : Nomenclature de la spécialité de formation du diplôme	83
Figure 18 : Nomenclature des MEF nationaux pour le MEF « 1CAP2 CHOCOLATIER CONFISEUR ».....	86
Figure 19 : Nomenclature des MEF nationaux pour le MEF « PREMIERE SCIENTIFIQUE SVT »	87
Figure 20 : Nomenclature des MEFSTAT nationaux pour le MEF « 1CAP2 CHOCOLATIER CONFISEUR ».....	89
Figure 21 : Nomenclature des MEFSTAT nationaux pour le MEF « PREMIERE SCIENTIFIQUE SVT ».....	90
Figure 22 : Nomenclature des matières enseignées pour l'enseignement « ALLEMAND LV1 ».....	92
Figure 23 : Nomenclature des disciplines pour la discipline de poste « ALLEMAND LETTRES ».....	93

Table des tableaux

Tableau 1: Exigences et recommandations concernant la mise en œuvre d'une fédération d'identités	15
Tableau 2: Exigences et recommandations concernant la propagation des informations d'identités hors ENT dans le cadre de la mise en œuvre d'une fédération d'identités.....	23
Tableau 3: Vecteur d'identité technique élève et représentant légal	25
Tableau 4: Exigences et recommandations pour les guichets et portails mis en œuvre par l'Éducation nationale.....	26
Tableau 5: Catégories de services Tiers hors périmètre GAR selon les conditions d'accès	28
Tableau 6: Autres attributs non associés à une identité pouvant être transmis pour les services de catégorie 2 et 3	31
Tableau 7: Exigences et recommandations concernant l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités	45
Tableau 8: Exemple de priorisation pour la reprise et la portabilité de données de l'ENT.....	66
Tableau 9: Exigences et recommandations concernant la stratégie d'exploitation.....	73
Tableau 10: Nomenclatures associées à la thématique de la formation	83
Tableau 11: Nomenclatures associées à la position de la formation dans le cursus	84
Tableau 12: Niveaux de rupture du MEFSTAT1.....	88
Tableau 13: Exemples d'informations disponibles à partir d'un MEF national.....	91
Tableau 14: Exemples de disciplines de recrutement et de disciplines de postes associées	93
Tableau 15: Nomenclatures transmises pour les élèves dans le second degré.....	98
Tableau 16: Nomenclatures transmises pour les enseignants de l'Éducation nationale dans le second degré.....	100
Tableau 17: Identifiants des profils de l'accédant.....	101
Tableau 18: Détermination du profil de l'accédant à partir de la classe d'objet et de la fonction....	102
Tableau 19: Combinaisons possibles des éléments resp et contact dans le champ ENTElevePersRelEleve	103
Tableau 20: Exigences et recommandations concernant les nomenclatures.....	104
Tableau 21: Exigences et recommandations concernant l'ensemble annuaire.....	113
Tableau 22: Exigences et recommandations relatives aux aspects juridiques.....	152

1. Introduction

1.1. Organisation du SDET

Pour connaître les versions en vigueur du SDET (document principal et annexe opérationnelle), consulter la [page de présentation du SDET](#)¹ sur le site éducol.

À partir de la version 6.0, le SDET est organisé en deux parties ayant des vocations différentes :

- un document principal ;
- une annexe opérationnelle.

Un glossaire est disponible dans le document principal.

Une **documentation d'accompagnement** en cours de constitution regroupe des documents pouvant servir d'exemples pour aider les projets ENT.



Figure 1 : Organisation du SDET et de la documentation d'accompagnement

¹ Page de présentation du SDET sur le site éducol (<http://eduscol.education.fr/sdet>)

1.2. Organisation de l'annexe opérationnelle

La présente **annexe opérationnelle** complète le document principal avec :

- des éléments opérationnels sur des sujets de mise en œuvre notamment annuaire, stratégie d'exploitation, authentification-autorisation-SSO², nomenclatures, médiacentre ;
- des éléments juridiques ;
- des grilles de conformité regroupant l'ensemble des exigences et recommandations identifiées à travers le SDET.

Elle est composée :

- du présent document ;
- des différents documents référencés aux chapitres 6 à 10.

1.3. Niveaux d'exigence des recommandations formulées



Figure 2 : Niveau d'exigence des recommandations

Comme dans le document principal, le niveau de recommandations formulé est exprimé en utilisant des termes issus de la terminologie [RFC2119](https://www.ietf.org/rfc/rfc2119.txt)³, notés en caractères gras et en majuscules dans le texte, dont la définition appliquée à ce document est la suivante :

- **DOIT** : ce mot signifie que la définition est une exigence absolue de la spécification (c'est-à-dire du présent document) ;
- **NE DOIT PAS** : cette expression signifie que la définition est une interdiction absolue de la spécification (c'est-à-dire du présent document) ;
- **DEVRAIT** : ce mot signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ne pas appliquer cette recommandation, mais les conséquences doivent être comprises et analysées soigneusement avant de choisir une autre option ;

² SSO : Single Sign-on (authentification unique)

³ RFC 2119 (<https://www.ietf.org/rfc/rfc2119.txt>)

- **NE DEVRAIT PAS** : cette expression signifie qu'il peut exister des raisons valables, dans des circonstances particulières, quand le comportement particulier est acceptable ou même utile, de ne pas suivre cette recommandation mais les conséquences doivent être comprises et le cas soigneusement pesé ;
- **PEUT** : ce mot exprime une suggestion ou proposition facultative.

Les recommandations sont formulées dans des tableaux aux chapitres 2 et 2.6.4 pour lesquels, en regard de chaque préconisation, une lettre rappelle le niveau d'exigence applicable à l'enseignement du premier degré ou du second degré ; la signification de cette lettre est la suivante :

- la lettre « E » pour « exigé » correspond à une exigence de type « **DOIT** » ou « **NE DOIT PAS** » ;
- la lettre « R » pour « recommandé » correspond à une recommandation de type « **DEVRAIT** » ou « **NE DEVRAIT PAS** » ;
- la lettre « F » pour « facultatif » correspond à une préconisation optionnelle de type « **PEUT** ».

2. Authentification– Autorisation–SSO (AAS)

2.1. Introduction

Ce chapitre de l'annexe opérationnelle SDET s'inscrit dans le cadre des qualités attendues d'un ENT au titre de la sécurité, particulièrement celles de la sécurité des accès et de la confidentialité des données.

Il complète la description de trois des services du domaine **services Socle Sécurité** de l'architecture de référence regroupés ici sous la dénomination **services AAS** ; en l'occurrence :

- le **service Identification et authentification** [SOC-SEC-IAU] ;
- le **service Autorisation** [SOC-SEC-AUT] ;
- le **service Propagation des informations d'identité** [SOC-SEC-PII].

À cet effet, il fournit un ensemble de définitions destinées à préciser certains concepts et des exigences et des recommandations à respecter afin que tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire évoluent dans un cadre de confiance autour de trois sujets d'attention principaux :

- la fédération d'identités ;
- la propagation des informations d'identité ;
- l'interfaçage entre l'ENT et les services externes au projet ENT (services Tiers) sans fédération d'identités.

2.2. Fédération d'identités

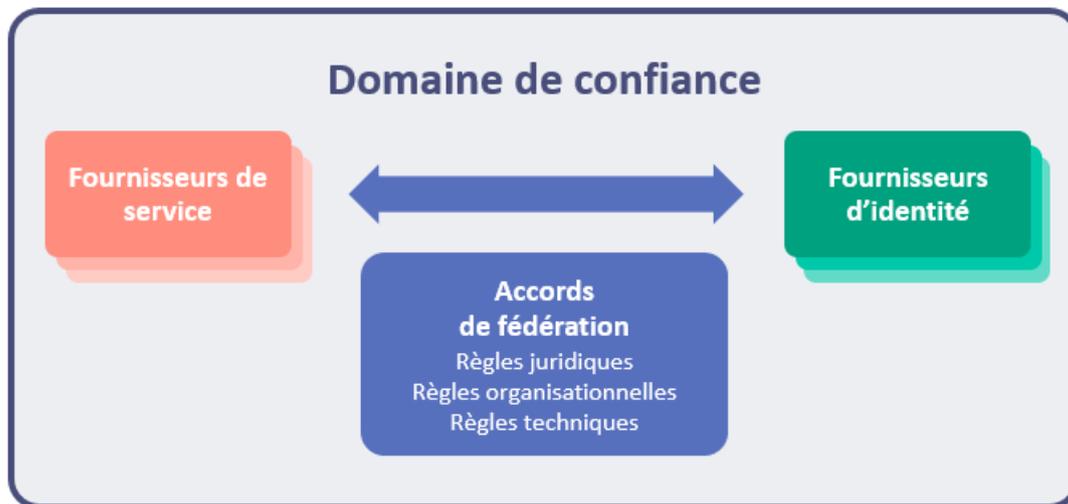


Figure 3 : Concepts clé de la fédération d'identités

La fédération d'identités s'articule autour des concepts clés suivants :

- domaine de confiance ;
- fournisseur d'identité ;
- fournisseur de service ;
- fournisseur d'attributs ;
- accords de fédération.

2.2.1. Domaine de confiance

Un **domaine de confiance** désigne l'ensemble des fournisseurs d'identité, des fournisseurs de services et des relations de confiance établies entre eux (pour leur permettre l'accès contrôlé et sécurisé aux différents services).

« Un espace de confiance est un ensemble de ressources, de services informatiques et de services de communication qui permettent des échanges dans des conditions de sécurité suffisantes et cohérentes » (Journal Officiel, 27/12/2009).

Voir aussi le chapitre « Cadre de confiance » dans le document principal.

2.2.2. Fournisseur d'identité

Le **fournisseur d'identité** se définit comme une composante de l'espace de confiance chargée de mettre à disposition un service d'identification pour les utilisateurs qui sont gérés dans son périmètre. Techniquement, le fournisseur d'identité assure l'authentification des utilisateurs et l'enrichissement du vecteur d'identification (par exemple : ajout d'attributs tels que la localisation ou le rôle fonctionnel de l'utilisateur).

2.2.3. Fournisseur de service

Le **fournisseur de service** se définit comme une composante de l'espace de confiance mettant des services applicatifs et des ressources à disposition des utilisateurs et des organisations autorisées. Il est également chargé de gérer l'autorisation d'accès aux ressources et aux applications. Le fournisseur de service peut s'appuyer sur le fournisseur d'identité pour les fonctions d'identification et d'authentification.

2.2.4. Fournisseur d'attributs

Un fournisseur d'identité peut être **fournisseur d'attributs** s'il envoie les données nécessaires au fournisseur de service pour la gestion des contrôles d'accès aux ressources ou la personnalisation des contenus.

2.2.5. Service de découverte du fournisseur d'identité

Le **Service de découverte du fournisseur d'identité**⁴ est une fonction d'aiguillage permettant de diriger l'utilisateur vers le fournisseur d'identité adéquat.

Ce service de découverte :

- présente à l'utilisateur **une liste de choix correspondant à des liens vers les fournisseurs d'identité** ;
- lui demande de choisir en fonction des caractéristiques qui lui correspondent ;
- et l'envoie vers la page de connexion du fournisseur d'identité choisi.

Une fonction de mémorisation du choix est souvent proposée (pour les utilisateurs qui utilisent systématiquement le même fournisseur d'identité).

⁴ Souvent abrégé en « service de découverte » ; parfois désigné sous l'acronyme anglais WAYF pour « where are you from ».

2.2.6. Accords de fédération

Le domaine de confiance de la fédération **DOIT** être régi par un ou des **accords de fédération**, mis en place par les porteurs de projet, en lien avec les différentes parties prenantes de la fédération. C'est cet accord qui définit les droits et devoirs des membres de la fédération.

Il contient les règles suivantes :

- identification des intervenants dans la fédération d'identités ;
- périmètre de fédération ;
- engagements du fournisseur d'identité ;
- identité et attributs produits ;
- engagements du fournisseur de service ;
- engagements réciproques ;
- durée de l'accord, principes de renouvellement et de rupture ;
- coûts.

Dans le cas d'une relation multiple (plusieurs fournisseurs de service / fournisseurs d'identité), l'accord peut être :

- global (mais validé et signé par chaque partie concernée) si le cycle de vie de la relation de fédération est identique et que les conditions et procédures de fédération sont identiques ; on retrouvera cette configuration dans le cas des relations intra Éducation nationale ;
- au cas par cas ; on pourra retrouver ce cas dans les relations entre l'Éducation nationale et un partenaire.

Les engagements suivants **DOIVENT** être pris par les **fournisseurs d'identité** et les **fournisseurs de service** :

- respect de l'objet et des règles communes de fonctionnement de la fédération ;
- gestion des identités et des autorisations selon des procédures formalisées et diffusées ;
- protection des données à caractère personnel ;
- respect de règles de sécurité ;
- utilisation des standards technologiques définis.

Les engagements suivants **DOIVENT** être pris par les **fournisseurs d'identité** :

- gestion des moyens d'authentification ;
- obligation réglementaire de traçabilité.

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

- définition, mise à jour et respect des données partagées ;
- définition le cas échéant d'une notion d'identifiant unique sur le périmètre de la fédération et de sa forme ;
- journalisation des usages du service d'identification / authentification.

La gouvernance de la fédération **DOIT** être assurée, notamment afin de :

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

La fédération **DOIT** être administrée, notamment afin de :

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

Les standards technologiques de la fédération **DOIVENT** être définis.

2.2.7. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Fédération d'identités	L'accord de fédération DOIT être mis en place par les porteurs de projet, en lien avec les différentes parties prenantes de la fédération.	E	E
02	Fédération d'identités	Les engagements suivants DOIVENT être pris par les fournisseurs d'identité et les fournisseurs de service : <ul style="list-style-type: none"> ■ respect de l'objet et des règles communes de fonctionnement de la fédération ; ■ gestion des identités et des autorisations selon des procédures formalisées et diffusées ; ■ protection des données à caractère personnel ; ■ respect de règles de sécurité ; ■ utilisation des standards technologiques définis. 	E	E
03	Fédération d'identités	Les engagements suivants DOIVENT être pris par les fournisseurs d'identité : <ul style="list-style-type: none"> ■ gestion des moyens d'authentification ; ■ obligation réglementaire de traçabilité. 	E	E
04	Fédération d'identités	Les engagements suivants PEUVENT être définis pour les fournisseurs d'identité : <ul style="list-style-type: none"> ■ définition, mise à jour et respect des données partagées ; ■ définition le cas échéant d'une notion d'identifiant unique sur le périmètre de la fédération et de sa forme ; ■ journalisation des usages du service d'identification / authentification. 	F	F
05	Fédération d'identités	La gouvernance de la fédération DOIT être assurée, notamment afin de : <ul style="list-style-type: none"> ■ définir l'organisation de la fédération ; ■ définir et faire vivre l'objet et les règles communes de fonctionnement de la fédération. 	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
06	Fédération d'identités	La fédération DOIT être administrée, notamment afin de : <ul style="list-style-type: none"> ▪ définir le statut administratif ; ▪ définir et distribuer les données partagées par tous les membres ; ▪ définir les orientations technologiques supportées (standards utilisés) et les règles de sécurité à suivre ; ▪ traiter les demandes d'inscription et de départ ; ▪ contrôler les engagements des membres de la fédération ; ▪ appliquer les évolutions des règles de fonctionnement. 	E	E
07	Fédération d'identités	Les standards technologiques de la fédération DOIVENT être définis.	E	E

Tableau 1 : Exigences et recommandations concernant la mise en œuvre d'une fédération d'identités

2.3. Propagation des informations d'identité entre l'ENT et les services externes au projet ENT

2.3.1. Généralités

Dans le cadre des projets ENT, la fédération d'identités concerne un ensemble d'acteurs de la sphère éducative (ministères, autorités académiques, collectivités territoriales ou autres organismes partenaires), qui coopèrent au sein d'un espace de confiance pour notamment gérer des identités, gérer les autorisations des utilisateurs et contrôler leurs accès.

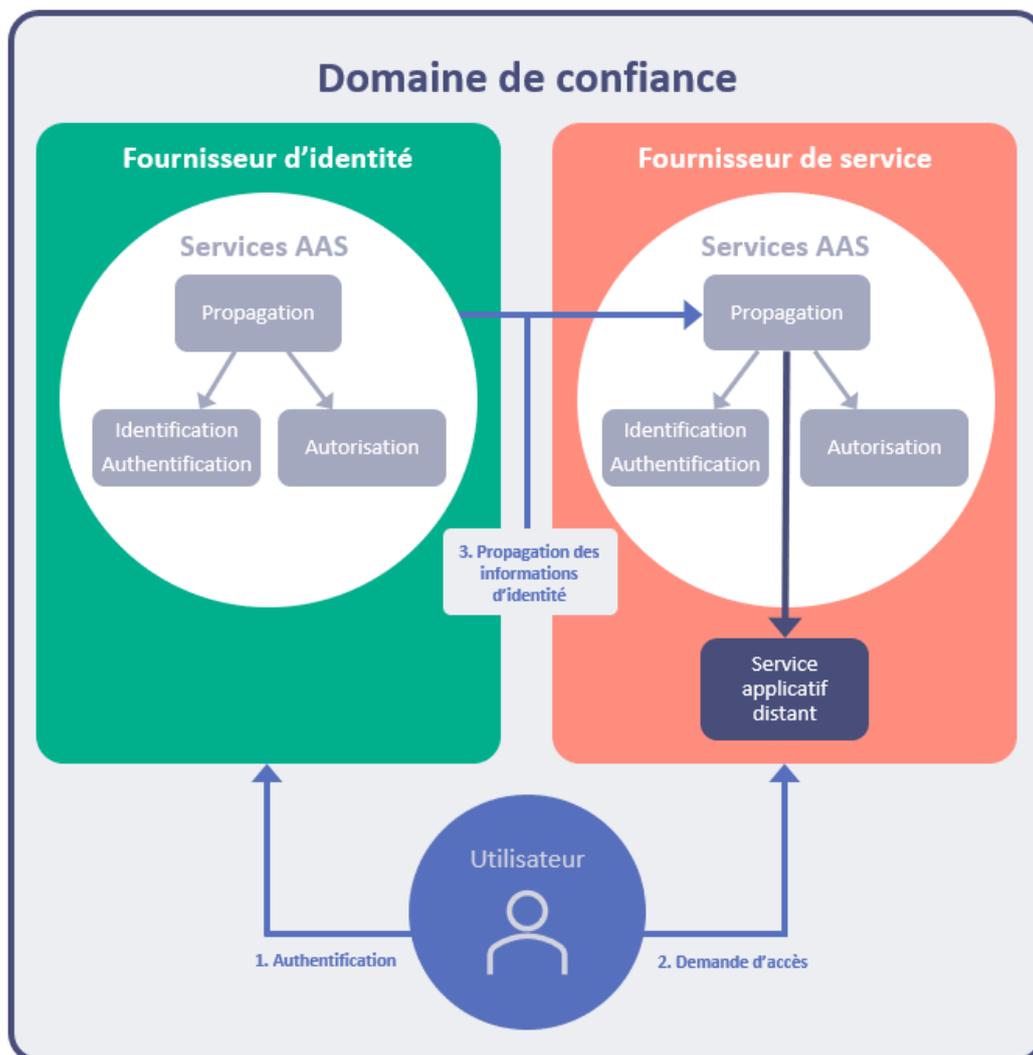
La solution ENT peut être fournisseur d'identité et/ ou fournisseur de service. Trois configurations peuvent se présenter :

- **ENT fournisseur d'identité et fournisseur de service** : c'est le cas « nominal » où l'utilisateur authentifié sur l'ENT accède aux services de ce même ENT ; la mise en œuvre des mécanismes de fédération d'identités n'est pas nécessaire ;
- **ENT fournisseur d'identité** : c'est le cas d'un utilisateur authentifié sur un ENT qui souhaite accéder à un service applicatif distant (externe au projet ENT), ce qui nécessite de transmettre des informations d'identité depuis l'ENT vers le fournisseur de service ; l'ENT joue ici le rôle de fournisseur d'identité, et éventuellement de fournisseur d'attributs ;

- **ENT fournisseur de service** : c'est le cas d'un utilisateur authentifié auprès d'un fournisseur d'identité externe qui souhaite accéder à un service applicatif proposé par l'ENT (ENT fournisseur de service) ; l'ENT reçoit de ce fournisseur d'identité des informations d'identité, sur la base desquelles le contrôle d'accès au service applicatif peut alors s'effectuer.

Ces cas d'usage sont illustrés sur la Figure 4 selon que l'on positionne la solution ENT en fournisseur d'identité ou de service :

- le fournisseur d'identité peut-être un ENT ou un fournisseur d'identité externe à l'ENT ;
- le fournisseur de service peut-être un ENT, un autre ENT ou un service externe à l'ENT.



* ENT 1 ou service d'authentification externe à l'ENT (exemple : guichet EN)

** ENT 1, ENT 2 ou service externe à l'ENT (exemple : guichet EN et services en ligne EN)

Figure 4 : Propagation des informations d'identité

Le domaine de confiance de la fédération est régi par le cadre général des règles de l'accord de fédération, qui déterminent notamment les engagements des fournisseurs d'identité et des fournisseurs de service.

Des compléments relatifs aux échanges d'informations d'identité sont donnés au chapitre 2.4 « Cas des guichets et des portails de service mis en œuvre par l' Education Nationale ».

2.3.2. Données partagées

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

En particulier, les attributs caractérisant les utilisateurs et nécessaires au contrôle des accès **DOIVENT** suivre un nommage et une sémantique communs au sein de la fédération.

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

2.3.3. Fonctions proposées

Le **service Propagation des informations d'identité** est décrit dans le chapitre « Architecture de référence ENT » du document principal du SDET.

2.3.4. Cinématiques d'accès

Ce chapitre présente les cinématiques d'accès pour différents cas d'usage.

Ces cinématiques ne sont pas exclusives les unes des autres et plusieurs d'entre elles peuvent se présenter au sein d'une même solution ENT, par exemple pour des profils utilisateurs différents.

2.3.4.1. ENT fournisseur de service

Dans les trois cas d'usage ci-après, l'ENT n'est pas fournisseur d'identité mais seulement fournisseur de service.

Il s'agit du cas de figure où l'identification / authentification des utilisateurs de l'ENT est déléguée à un guichet externe (par exemple : un guichet de l'Éducation nationale pour les personnels de l'Éducation nationale, pour les élèves et leurs responsables dans certains cas, un guichet de la collectivité pour un personnel de collectivité).

En cas de mise en œuvre d'une délégation d'authentification à un fournisseur d'identité externe, le portail de l'ENT **DOIT** être le point d'accès privilégié aux différents services de l'ENT. Des liens **DOIVENT** être prévus entre l'ENT et les services externes afin de faciliter les usages.

2.3.4.1.1. Cas d'usage : accès à un service ENT depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès dans le cas où l'utilisateur accède à l'ENT depuis le portail de l'ENT.

Remarque : ce cas d'usage ne peut pas s'appliquer à tous les utilisateurs de l'ENT : les comptes invités ou les catégories d'utilisateurs n'ayant pas de fournisseur d'identité externe doivent s'authentifier sur l'ENT.

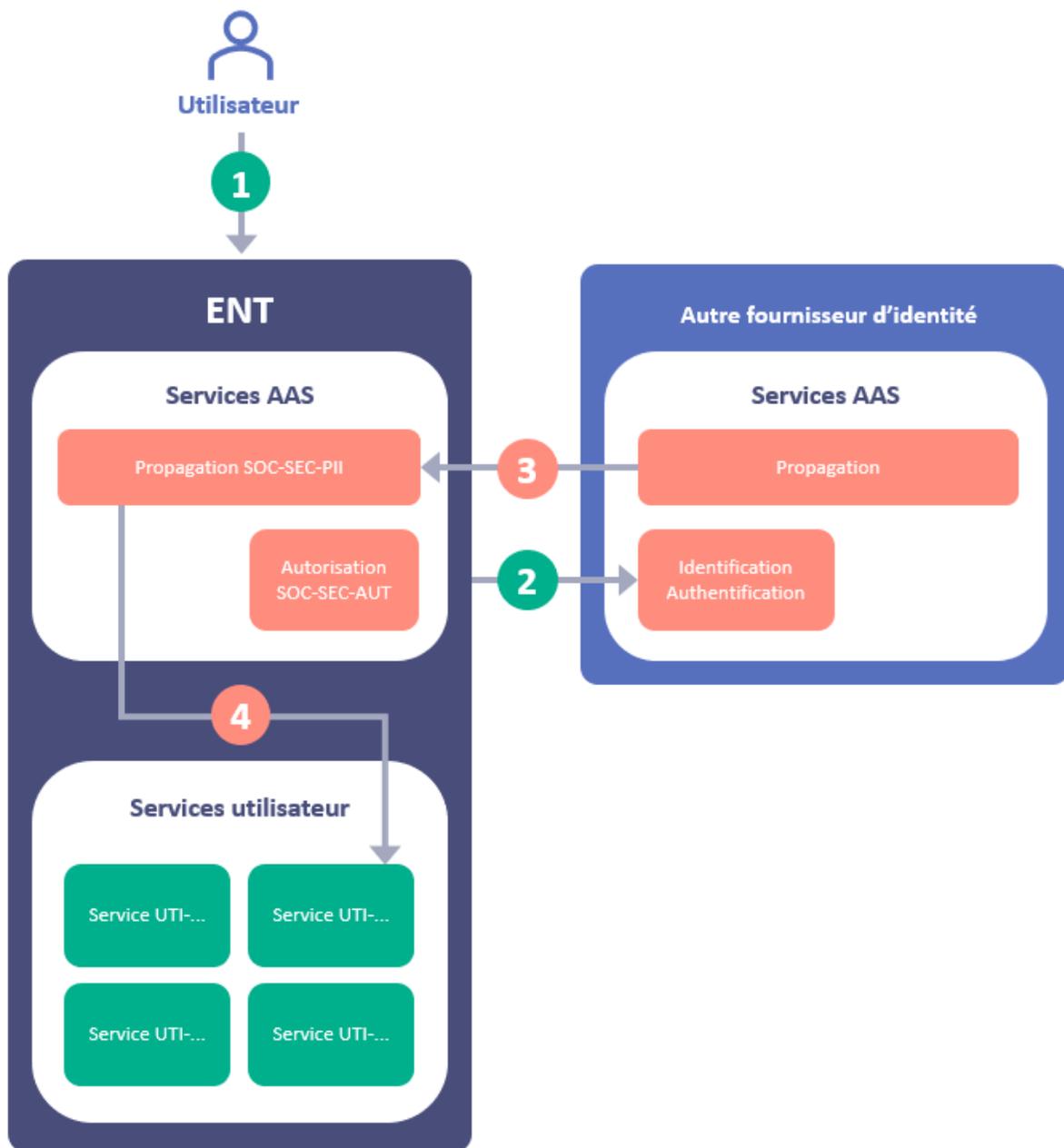


Figure 5 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 5 est la suivante :

- 1) l'utilisateur non authentifié accède à l'ENT ;
- 2) il indique son profil (élève, parent, enseignant...) sur le service de découverte de l'ENT ; il est redirigé vers le guichet d'authentification externe adéquat auprès duquel il s'authentifie ;
- 3) le guichet externe propage les informations d'identités vers l'ENT ;
- 4) le service de propagation de l'ENT propage ces informations vers le service applicatif de l'ENT.

L'utilisateur peut alors accéder aux services Utilisateurs de l'ENT auxquels il a droit.

2.3.4.1.2. Cas d'usage : accès à un service externe depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur travaille sur l'ENT et souhaite accéder aux services associés à son fournisseur d'identité (par exemple : ENT proposant un lien vers les services en ligne du ministère en charge de l'Éducation nationale pour les élèves et leurs représentants légaux, ceux-ci ayant été préalablement authentifiés auprès d'un guichet de l'Éducation nationale).

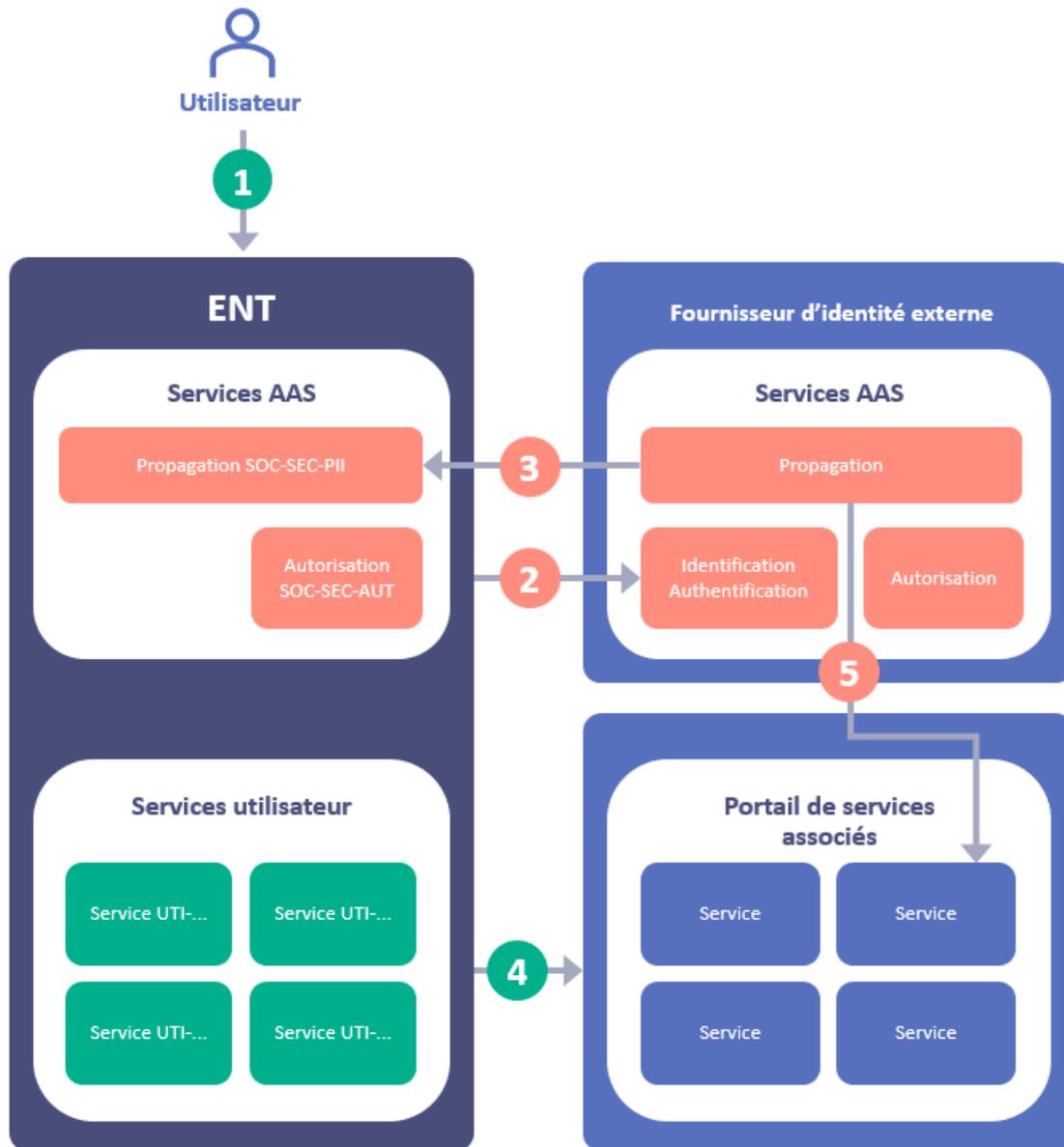


Figure 6 : Authentification déléguée à un fournisseur d'identité externe et accès à un fournisseur de service externe depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 6 est la suivante :

- 1) l'utilisateur non authentifié accède à l'ENT ;
- 2) il indique son profil (élève, parent, enseignant, agent...) sur le service de découverte de l'ENT ; il est redirigé vers le guichet d'authentification externe auprès duquel il s'authentifie ;
- 3) le guichet externe propage les informations d'identités vers l'ENT ;

- 4) l'utilisateur choisit dans son ENT un lien vers un service associé au guichet externe ; le service de propagation du guichet externe propage les informations d'identité vers le portail de services associé.

L'utilisateur peut alors accéder au service externe, selon ses droits.

2.3.4.1.3. Cas d'usage : accès à un service ENT depuis un portail externe

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur utilise les services associés à son fournisseur d'identité, et souhaite accéder à l'ENT (par exemple : portails académiques ou portails des collectivités proposant un lien vers le portail de l'ENT).

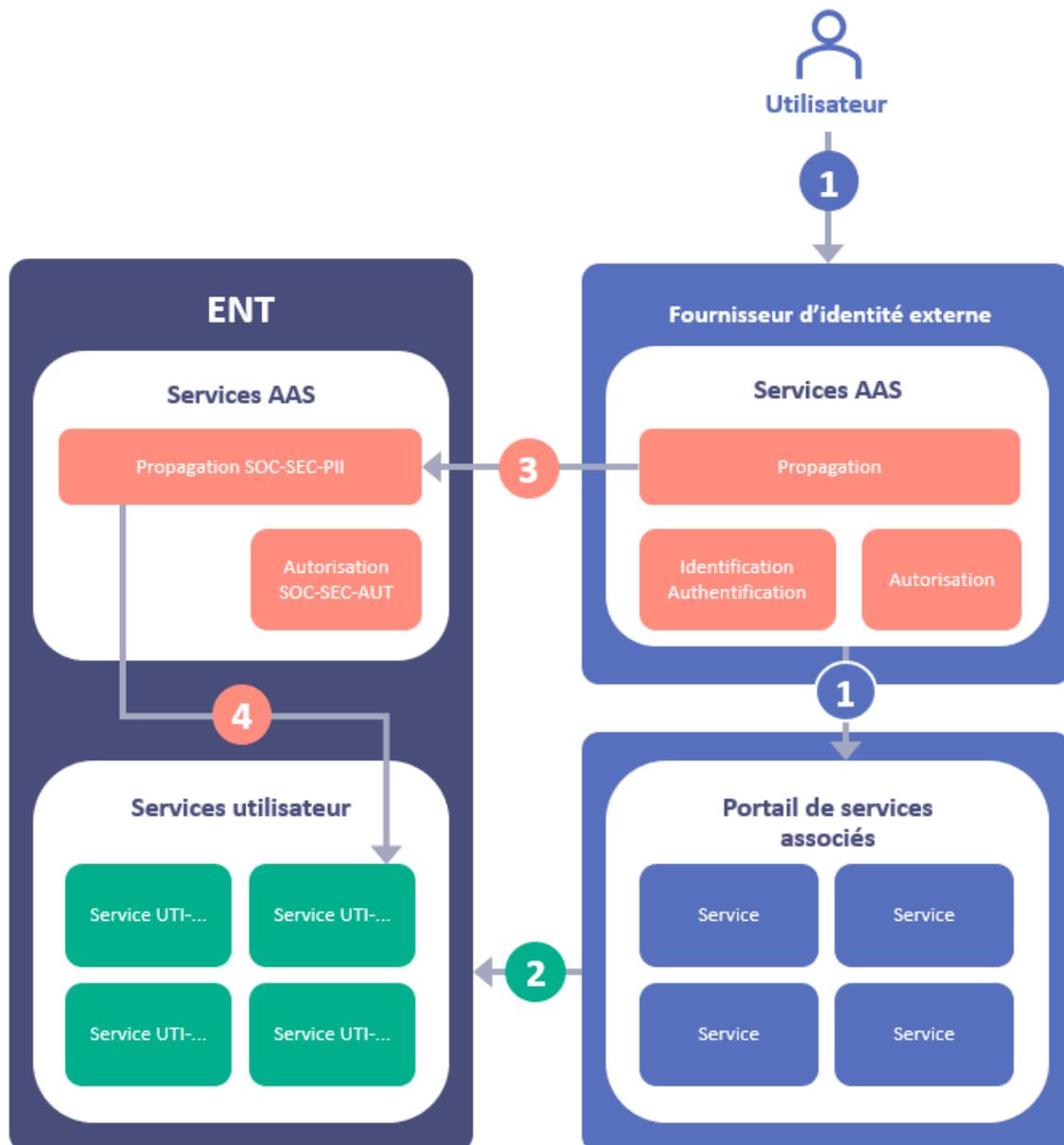


Figure 7 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis un portail externe

La cinématique d'accès indiquée à la Figure 7 est la suivante :

- 1) l'utilisateur non authentifié accède au portail de services associé à son fournisseur d'identité ; il s'authentifie auprès du guichet et a accès aux services proposés sur le portail ;
- 2) l'utilisateur sélectionne le lien vers le portail de l'ENT ;
- 3) le guichet externe propage les informations d'identité vers l'ENT ;
- 4) le service de propagation de l'ENT propage ces informations vers le service applicatif de l'ENT.

L'utilisateur peut alors accéder aux services Utilisateurs de l'ENT auxquels il a droit.

2.3.4.2. ENT fournisseur d'identité

Dans le cas d'usage illustré Figure 8, l'ENT est le fournisseur d'identité.

2.3.4.2.1. Cas d'usage : accès à un service externe dans un domaine de confiance depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur, préalablement authentifié sur son ENT et utilisant les services de l'ENT, souhaite accéder à des services externes en mode de fédération d'identités (par exemple : l'accès aux fonctions d'affectation du GAR⁵ par le délégué affectation, l'accès aux ressources pédagogiques éditoriales via le GAR depuis le **Médiacentre** de l'ENT, l'accès aux services en ligne du ministère en charge de l'Éducation nationale pour les élèves et leurs représentants légaux dans certains cas).

⁵ GAR (Gestionnaire d'accès aux ressources)

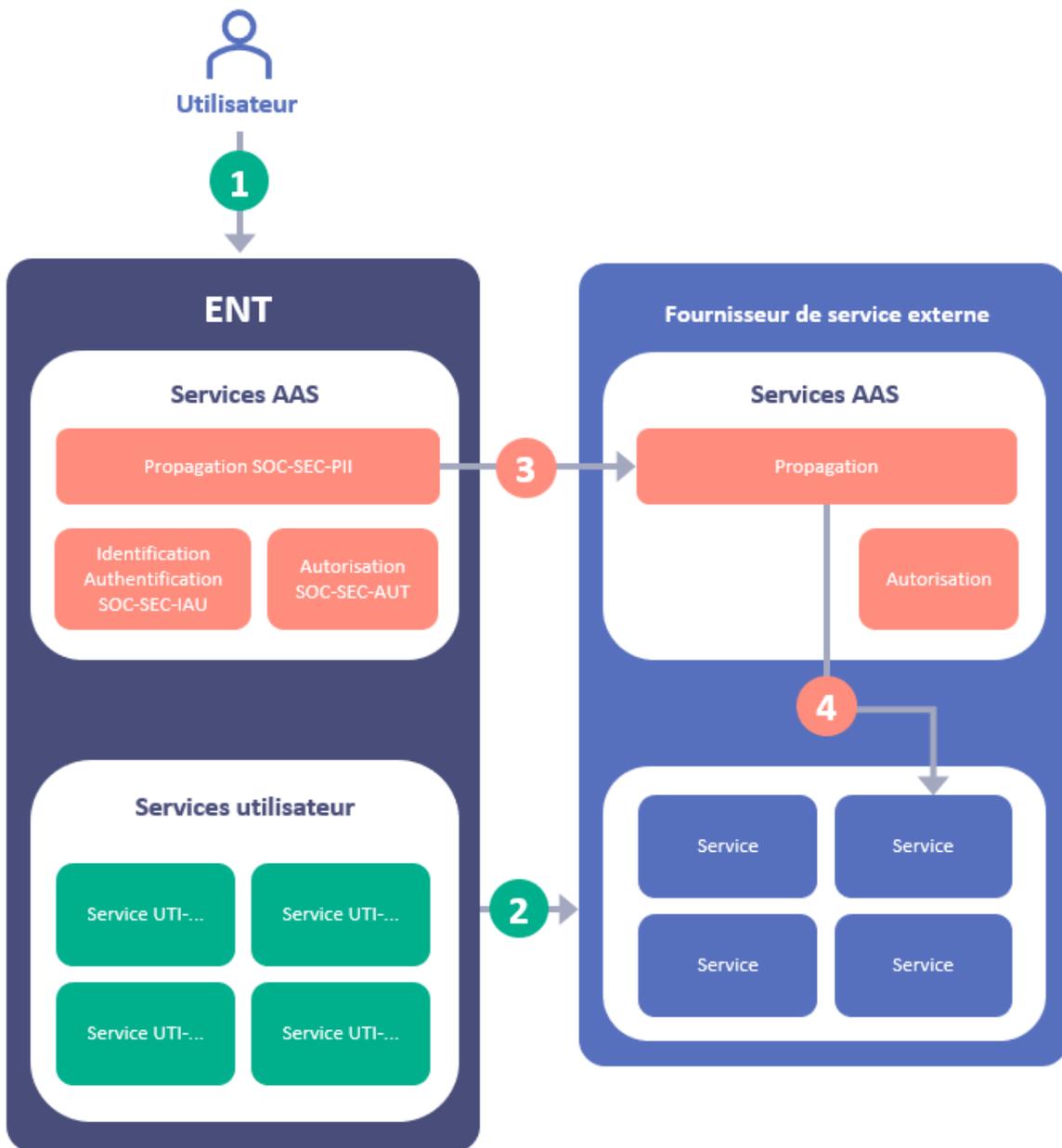


Figure 8 : ENT fournisseur d'identité et accès à un service externe depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 8 est la suivante :

- 5) l'utilisateur s'authentifie sur l'ENT ;
- 6) l'utilisateur sélectionne le lien vers le service externe ;
- 7) l'ENT propage les informations d'identité vers le fournisseur de service externe ;
- 8) l'utilisateur peut alors accéder au service externe.

2.3.5. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Propagation des informations d'identité hors ENT	Les attributs caractérisant les utilisateurs et nécessaires au contrôle des accès DOIVENT suivre un nommage et une sémantique communs au sein de la fédération. Les moyens d'authentification partagés DOIVENT être définis de manière commune dans toute la fédération.	E	E
02	Délégation d'authentification	En cas de mise en œuvre d'une délégation d'authentification à un fournisseur d'identité externe, le portail de l'ENT DOIT être le point d'accès privilégié aux différents services de l'ENT. Des liens DOIVENT être prévus entre l'ENT et les services externes afin de faciliter les usages.	E	E

Tableau 2 : Exigences et recommandations concernant la propagation des informations d'identités hors ENT dans le cadre de la mise en œuvre d'une fédération d'identités

2.4. Cas des guichets et des portails de service mis en œuvre par l'Éducation nationale

Les configurations et cinématiques d'accès évoquées peuvent s'appliquer aux portails de services et aux guichets d'authentification proposés par le ministère :

- le portail « Scolarité Services » du ministère en charge de l'Éducation nationale ;
- les autres portails académiques ;
- les guichets d'authentification académiques Agents pour les personnels de l'Éducation nationale ;
- le guichet national ÉduConnect pour les élèves et leurs représentants légaux.

Le ministère en charge de l'Éducation nationale et les académies ont pour ambition d'atteindre un niveau d'engagement de service des guichet équivalent à celui exigé des prestataires de la solution ENT.

Ceci suppose :

- la mise en cohérence et une bonne synchronisation des référentiels de données sur lesquels s'appuient les guichets et les annuaires ENT ;
- une qualité de service équivalente à celle du projet ENT ;
- des outils de supervision et de suivi de la qualité de service ;
- une capacité de tests pour la bonne articulation entre chaque projet ENT et le guichet ;

- le fait que le renforcement des services de l'Éducation nationale ne conduise pas à une redondance ou à une incohérence fonctionnelle entre les bouquets de service ;
- le maintien de l'ENT comme point d'accès privilégié aux différents services de l'ENT ;
- le lien entre l'ENT et les services de l'Éducation nationale.

2.4.1. Agents

2.4.1.1. Configurations possibles

Le guichet d'authentification de l'Éducation nationale pour les agents (guichet Agents) fournit les services d'identification, authentification et gestion des comptes utilisateurs associés.

La solution ENT peut s'articuler en fédération d'identités avec ces services et ce guichet selon les différentes configurations indiquées au chapitre 2.3.4 « Cinématiques d'accès ».

2.4.1.2. Données échangées

Une seule donnée **DOIT** être échangée : l'adresse email académique, l'attribut transmis devant être nommé **mail**.

2.4.2. Élèves et représentants légaux des élèves

2.4.2.1. Configurations possibles

Le guichet national ÉduConnect fournit les services d'identification, authentification et gestion des comptes utilisateurs associés pour les représentants légaux et les élèves.

La solution ENT peut s'articuler en fédération d'identités avec les services en ligne du ministère en charge de l'Éducation nationale et ce guichet selon les différentes configurations indiquées au chapitre 2.3.4 « Cinématiques d'accès ».

2.4.2.2. Vecteur d'identité technique

Lors de la mise en œuvre du guichet national EduConnect, un vecteur d'identité technique commun pour les élèves et les représentants légaux et pérenne d'une année scolaire sur l'autre est proposé par le ministère en charge de l'Éducation nationale aux projets ENT conformes au SDET.

Le tableau ci-dessous décrit le format de ce vecteur d'identité utilisé :

Nom de l'attribut	Format	Nom de l'attribut dans l'annuaire ENT	Multivalué	Description
FrEduCtId	String	inexistant	N	Valeur chiffrée de l'identifiant interne EduConnect, constant dans le temps pour le périmètre d'un ENT
FrEduCtRefId	String	ENTPersonRefId	O	Identifiant dont l'étiquette détermine la provenance : <ul style="list-style-type: none"> ▪ une valeur préfixée par {ECT} contenant la valeur du FrEduCtId ▪ une ou plusieurs valeur(s) préfixée(s) par {AAF} (1 par identifiant de l'utilisateur dans les différents annuaires fédérateurs) contenant un triplet : <ul style="list-style-type: none"> ○ code BCN de l'académie (ex : 14 pour Rennes) ; la nomenclature BCN utilisée est N_ACADEMIE_ET_ASSIMILE ○ degré (AC1D ou AC2D) ○ identifiant de l'utilisateur dans l'annuaire fédérateur ▪ une valeur préfixée par {ECT-ENT} : valeur chiffrée de l'identifiant interne ECT, commune pour tous les ENT (salée avec un hash de la chaîne "ENT")

Tableau 3 : Vecteur d'identité technique élève et représentant légal

Exemples de valeurs :

- pour un parent d'élève avec un seul enfant scolarisé dans le second degré, le vecteur d'identité sera de la forme :

```
FrEduCtId :123456780034355445
FrEduCtRefId :{ECT}123456780034355445
FrEduCtRefId :{AAF} 18|AC2D|123456987
FrEduCtRefId : {ECT-ENT}91a51328d5b844d41fb7cdfc74831bc053bcb491889ba182a11d
6b7ee1e60cf30843ed055e6ce67b24899e0dd1d6830
```

- pour un parent d'élève avec trois enfants scolarisés dans le second degré, dont deux dans le même établissement, le vecteur d'identité sera de la forme :

```
FrEduCtId :123456780034355445
FrEduCtRefId :{ECT}123456780034355445
FrEduCtRefId :{AAF} 18|AC2D|123456987
FrEduCtRefId :{AAF} 18|AC2D|123445672
FrEduCtRefId : :{ECT-ENT}bc053bcb491889ba182a11d 91a51328d5b844d41fb7cdfc7483
6ce67b24899e0dd1d68306b7ee1e60cf30843ed0551e
```

- pour un parent d'élève avec deux enfants scolarisés dans le second degré dans 2 académies, le vecteur d'identité sera de la forme :

```
FrEduCtId :123456780034355445
FrEduCtRefId :{ECT}123456780034355445
FrEduCtRefId :{AAF} 18|AC2D|123456987
FrEduCtRefId :{AAF} 14|AC2D|568945782
```

FrEduCtRefId : :{ECT-ENT}cdfc74831bc053bcb491889ba182a11d 91a51328d5b844d416b7ee1e60cf30843ed055e6ce67b24899e0dd1d6830 fb7

- pour un élève scolarisé dans le second degré, le vecteur d'identité sera de la forme :

FrEduCtId :1234567800343333434

FrEduCtRefId :{ECT}1234567800343333434

FrEduCtRefId :{AAF} 18|AC2D|7899767786

FrEduCtRefId : :{ECT-ENT} d5b844d41fb7cdfc7483 bc053bcb491889ba182a11d 91a5286ce67b24899e0dd1d68306b7ee1e60cf30843ed0551e13

L'ENT **DOIT** être en mesure d'interpréter le vecteur d'identité élève et représentant légal dans le format du vecteur d'identité technique et de faire le lien avec le compte utilisateur.

2.4.3. Récapitulatif des exigences et des recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Propagation informations d'identité hors ENT / agent	Propagation d'identité avec le guichet des agents : une seule donnée DOIT être échangée : l'adresse email académique - l'attribut transmis devant être nommé mail .	E	E
03	Propagation informations d'identité hors ENT / élèves	L'ENT DOIT être en mesure d'interpréter le vecteur d'identité élève et représentant légal dans le format du vecteur d'identité technique et de faire le lien avec le compte utilisateur.	E	E
04	Propagation informations d'identité hors ENT / représentants légaux	L'ENT DOIT être en mesure d'interpréter le vecteur d'identité « parent » (représentant légal) dans le format profil Nom Prenom levelId UaiEtab ou FrEduCtId FrEduCtRefId et de faire le lien avec le compte utilisateur	E	E
05	Propagation informations d'identité hors ENT	La solution ENT DEVRAIT mettre en œuvre des traitements qui permettent d'identifier l'établissement auquel l'utilisateur peut accéder.	R	R

Tableau 4 : Exigences et recommandations pour les guichets et portails mis en œuvre par l'Éducation nationale

2.5. Cas du guichet d'authentification de l'enseignement agricole

Le guichet d'authentification de l'enseignement agricole fournit le service d'identification, d'authentification et de gestion des comptes utilisateur pour les agents, les apprenants⁶ et les personnes en lien avec les apprenants (« responsables »). Il s'agit du guichet unique pour les trois populations.

Le vecteur d'identité **FrEduVecteur** retourné par le guichet de l'enseignement agricole contient la clé de jointure de la personne (valeur de l'attribut `ENTPersonJointure`).

2.6. Exigences et recommandations pour l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités

Ce chapitre apporte des exigences et des recommandations opérationnelles dans le cadre de l'interfaçage entre la solution ENT et des services applicatifs Tiers (hors services en ligne du ministère en charge de l'Éducation nationale et hors GAR). Quelle que soit la catégorie de services Tiers, la solution ENT est considérée comme fournisseur d'identité.

Selon le type d'interface fonctionnelle entre une solution ENT et un service Tiers, plusieurs catégories de services Tiers peuvent être définies. Des recommandations spécifiques à chaque catégorie sont données ci-après.

Le chapitre est organisé comme suit :

- la première partie présente les différentes catégories de services Tiers ;
- la deuxième partie précise, pour chaque catégorie, des exigences et recommandations opérationnelles notamment en termes de données pouvant être transmises par la solution ENT au service Tiers ;
- la troisième partie rappelle la nécessité de la mise en place d'une convention de service entre le projet ENT et le service Tiers et présente les différents sujets devant être traités dans une telle convention ;
- la quatrième partie récapitule les exigences et recommandations liées à l'interfaçage avec les services Tiers.

⁶ Dans l'enseignement agricole, les apprenants comportent les élèves, les apprentis et les adultes en formation continue.

2.6.1. Présentation des différentes catégories de services Tiers

La définition des catégories de services Tiers repose sur les caractéristiques fonctionnelles de l'interface entre le service Tiers et l'ENT, et notamment les modalités d'authentification et de contrôle d'accès, le type d'informations d'identité transmises et le stockage ou non de ces informations par le service Tiers.

Les services Tiers sont ainsi répartis en cinq catégories, dont les caractéristiques sont présentées dans le tableau ci-après :

Catégorie de services Tiers hors GAR	Conditions d'accès
Catégorie 1	L'accès au service ne nécessite ni authentification ni contrôle d'accès (accès libre).
Catégorie 2	L'accès au service nécessite une authentification et un contrôle d'accès basés uniquement sur l'appartenance de l'utilisateur au projet ENT et/ou à une école ou un établissement scolaire défini et/ou à son profil d'accédant ⁷ .
Catégorie 3	L'accès au service nécessite une authentification et un contrôle d'accès de l'accédant avec transmission de données uniques par utilisateur mais non nominatives (identifiant utilisateur non significatif).
Catégorie 4	L'accès au service s'effectue sur la base d'informations non nominatives transmises par l'ENT lors de la connexion et sur la base d'informations nominatives sur l'accédant, dont dispose au préalable le service Tiers (« mapping » d'identités réalisé par le service Tiers). Le processus préalable d'inscription au service applicatif Tiers s'effectue hors ENT.
Catégorie 5	L'accès au service s'effectue sur la base d'informations fournies par l'utilisateur lors de la première connexion au service Tiers via l'ENT (formulaire en ligne...). Lors des connexions suivantes, l'accédant sera reconnu par le service Tiers sur la base d'informations utilisateur transmises par l'ENT (fonctionnement identique à la catégorie 4 : mapping d'identités).

Tableau 5 : Catégories de services Tiers hors périmètre GAR selon les conditions d'accès

2.6.2. Exigences et recommandations fonctionnelles

Pour chaque catégorie de services Tiers citée ci-dessus, les éléments suivants seront détaillés :

- la cinématique fonctionnelle ;
- les données potentiellement transmises.

En tout état de cause, le principe de proportionnalité défini par la CNIL relatif à la protection des données personnelles doit être respecté : *« seules doivent être enregistrées les informations pertinentes et nécessaires pour leur finalité. »*.

Les données transmises ne peuvent pas être utilisées à d'autres finalités de traitement que celles indispensables à la fourniture du service.

⁷ Le profil de l'accédant est défini au chapitre 5.7 « Profils de l'accédant »

2.6.2.1. Services de catégorie 1

Rappel : l'accès à un service de catégorie 1 ne nécessite ni authentification ni contrôle d'accès (accès libre).

2.6.2.1.1. Cinématique fonctionnelle

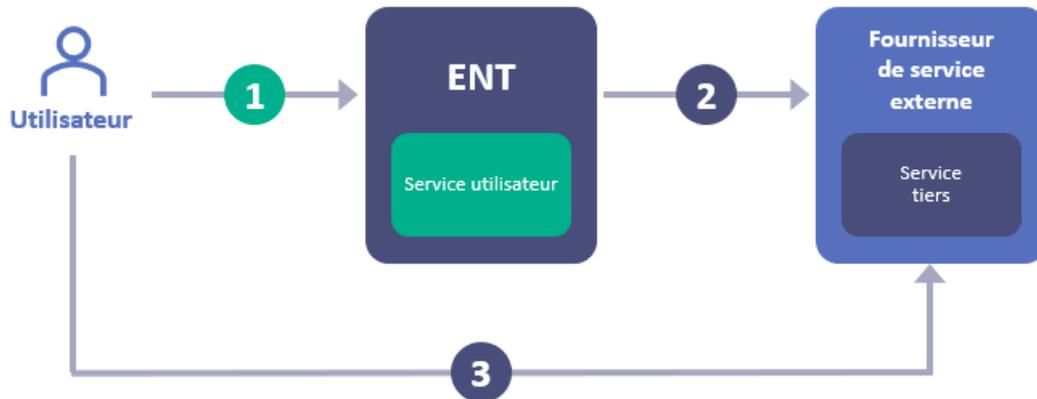


Figure 9 : Cinématique fonctionnelle pour les services de catégorie 1

Comme illustré Figure 9, la cinématique d'accès à un service de la catégorie 1 est la suivante :

- 1) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) l'utilisateur accède de façon anonyme au service Tiers sans qu'aucune information ne soit nécessaire pour le contrôle d'accès au niveau du service Tiers.

2.6.2.1.2. Données transmises

La solution ENT **NE DOIT PAS** transmettre d'informations d'identité sur l'utilisateur à un service Tiers de catégorie 1.

2.6.2.1.3. Exemple

Un utilisateur accède à un site internet qu'il a déposé dans ses favoris de l'ENT, par activation du lien.

Aucune donnée n'est envoyée par l'ENT au site externe. L'utilisateur change de sphère de responsabilité et de configuration de travail.

2.6.2.2. Services de catégorie 2

Rappel : l'accès à un service de catégorie 2 nécessite une authentification et un contrôle d'accès basés uniquement sur l'appartenance de l'utilisateur au projet ENT et/ou à une école ou un établissement scolaire défini et/ou à son profil d'accédant.

2.6.2.2.1. Cinématique fonctionnelle

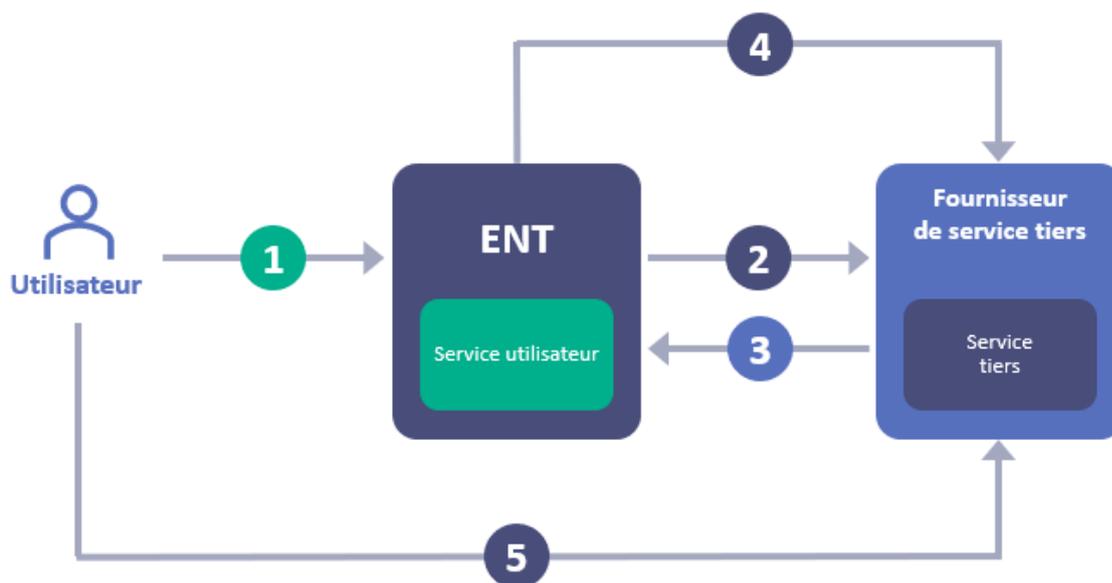


Figure 10 : Cinématique fonctionnelle pour les services de catégorie 2

Comme illustré Figure 10, la cinématique d'accès à un service de la catégorie 2 est la suivante :

- 1) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
 - a) l'identification et le contrôle d'accès sont effectués par le service Tiers sur la base de l'appartenance de l'utilisateur au projet ENT et/ou à une école ou à un établissement et/ou à son profil d'accédant ;
 - b) d'autres attributs non associés à une identité décrits dans le Tableau 6 peuvent être transmis également uniquement s'ils sont indispensables au fonctionnement du service Tiers ;
- 4) la solution ENT fournit au service Tiers les informations demandées à l'étape précédente ;
- 5) l'utilisateur accède de façon anonyme au service Tiers.

2.6.2.2.2. Données transmises

Les données qui PEUVENT être transmises par la solution ENT afin d'assurer l'authentification et le contrôle d'accès sont :

- l'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. chapitre 5.2 « Codes des projets ENT ») ;
- l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé (la solution ENT doit mettre en œuvre des traitements qui permettent d'identifier l'établissement auquel l'utilisateur accède dans l'ENT) ;
- le profil de l'accédant, non associé à une identité (cf. chapitre 5.7 « Profils de l'accédant »).

De plus d'autres attributs non associés à une identité **PEUVENT** être transmis **uniquement s'ils sont indispensables au fonctionnement du service Tiers**. Ces attributs sont décrits dans le Tableau 6 et les définitions associées à ces attributs sont disponibles dans les annexes de l'ensemble annuaire (cf. chapitre 8 « Ensemble annuaire »).

Toute autre donnée **NE DOIT PAS** être transmise.

Profil de l'accédant	Attributs 1er degré	Attributs 2 nd degré	Nomenclatures BCN correspondantes
National_elv	Niveau de formation	Niveau de formation	N_MEF_STAT_4
National_elv	(N/A)	Filière	N_MEF_STAT_5
National_elv	(N/A)	Niveau de formation du diplôme	N_NIVEAU_FORMATION_DIPLOME
National_elv	(N/A)	Spécialité du diplôme	N_FORMATION_DIPLOME
National_elv	(N/A)	Enseignements	N_MATIERE_ENSEIGNEE
National_elv	Classe	Classe	Pas de nomenclature nationale
National_elv	Groupe(s)	Groupe(s)	Pas de nomenclature nationale
National_ens	Spécialité de poste	Discipline de poste	N_DISCIPLINE_POSTE / N_SPECIALITE_POSTE
National_ens	(N/A)	Matières enseignées	N_MATIERE_ENSEIGNEE
National_ens	Classe(s)	Classe(s)	Pas de nomenclature nationale
National_ens	Groupe(s)	Groupe(s)	Pas de nomenclature nationale
National_tut	Aucun	Aucun	(N/A)
National_dir	(N/A)	Service	N/A
National_eta	(N/A)	Service	N/A
National_aca	(N/A)	Service	N/A
National_col	(N/A)	Service	N/A

Tableau 6 : Autres attributs non associés à une identité pouvant être transmis pour les services de catégorie 2 et 3

Des traitements doivent être réalisés par les solutions ENT afin de ne transmettre que les données relatives à l'établissement à partir duquel le service Tiers est appelé.

Par exemple, la solution ENT peut proposer à l'utilisateur, sur la base de l'attribut multivalué ENTPersonClasses (pour les élèves du premier degré), ENTEleveClasses (pour les élèves du second degré) ou l'attribut multivalué ENTPersonFonctions (pour les enseignants), une liste déroulante contenant les écoles / établissements auxquels il peut accéder. L'utilisateur sélectionne alors l'école / établissement dans lequel il souhaite travailler. En conséquence, lors de l'accès au service distant via l'ENT, c'est le code UAI de cette école ou de cet établissement qui sera transmis.

De même, certains enseignants exercent dans plusieurs établissements et certains élèves peuvent suivre des enseignements dans plusieurs établissements. La solution ENT devra alors faire les traitements nécessaires pour n'envoyer que la classe ou les groupes correspondant au code UAI sélectionné.

2.6.2.2.3. Exemple

Un utilisateur accède à une ressource pour laquelle son établissement a souscrit un abonnement.

Seul le code UAI est nécessaire si tous les usagers de l'établissement ont les mêmes autorisations sur la ressource. S'il y a des autorisations différentes par profil (par exemple pour les enseignants ou les élèves), la solution ENT peut également transmettre le profil de l'accédant.

2.6.2.3. Services de catégorie 3

Rappel : L'accès à un service de catégorie 3 nécessite une authentification et un contrôle d'accès de l'accédant avec **transmission de données uniques par utilisateur mais non nominatives** (identifiant utilisateur non significatif).

2.6.2.3.1. Cinématique fonctionnelle

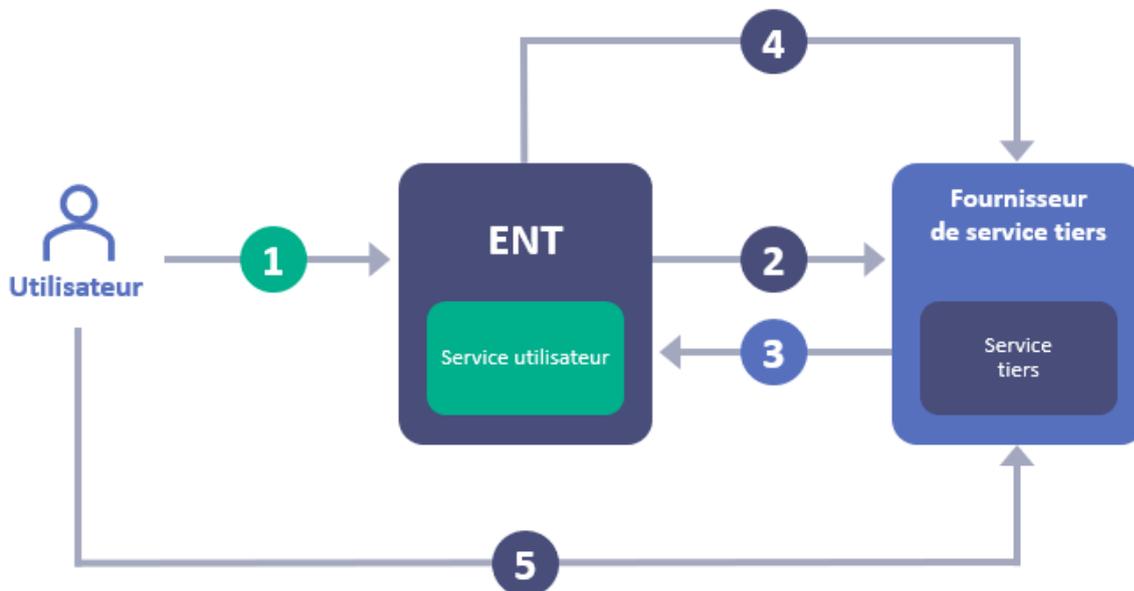


Figure 11 : Cinématique fonctionnelle pour les services de catégorie 3

Comme illustré Figure 11, la cinématique d'accès à un service de la catégorie 3 est la suivante :

- 1) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
 - a) l'authentification et le contrôle d'accès sont effectués par le service Tiers sur la base d'un **identifiant unique par utilisateur mais non nominatif et éventuellement de l'appartenance de l'utilisateur au projet ENT et/ou à une école ou à un établissement et/ou à son profil d'accédant** ;
 - b) d'autres attributs non associés à une identité décrits dans le Tableau 6 peuvent être transmis également uniquement s'ils sont indispensables au fonctionnement du service Tiers ;
- 4) l'ENT fournit au service Tiers les informations demandées à l'étape précédente ;

- 5) l'utilisateur accède de façon anonyme au service Tiers mais personnalisée au vu de l'identifiant utilisateur transmis.

2.6.2.3.2. Données transmises

Les données qui PEUVENT être transmises afin d'assurer l'authentification et le contrôle d'accès sont :

- un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant⁸ ;
- l'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. chapitre 5.2 « Codes des projets ENT ») ;
- l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ;
- le profil de l'accédant non associé à une identité (cf. chapitre 5.7 « Profils de l'accédant »).

De plus d'autres attributs non associés à une identité PEUVENT être transmis **uniquement s'ils sont indispensables au fonctionnement du service Tiers**. Ces attributs sont donnés dans le Tableau 6 et les définitions associées à ces attributs sont disponibles dans les annexes de l'ensemble annuaire (cf. chapitre 7 « Ensemble annuaire »).

Toute autre donnée **NE DOIT PAS** être transmise.

Des traitements doivent être réalisés par les solutions ENT afin de ne transmettre que les données relatives à l'établissement à partir duquel le service Tiers est appelé.

Par exemple, la solution ENT peut proposer à l'utilisateur, sur la base de l'attribut multivalué ENTPersonClasses (pour les élèves du premier degré), ENTEleveClasses (pour les élèves du second degré) ou l'attribut multivalué ENTPersonFonctions (pour les enseignants), une liste déroulante contenant les écoles / établissements auxquels il peut accéder. L'utilisateur sélectionne alors l'école / établissement dans lequel il souhaite travailler. En conséquence, lors de l'accès au service distant via l'ENT, c'est le code UAI de cette école ou de cet établissement qui sera transmis.

De même, certains enseignants exercent dans plusieurs établissements et certains élèves peuvent suivre des enseignements dans plusieurs établissements. La solution ENT devra alors faire les traitements nécessaires pour n'envoyer que la classe ou les groupes correspondant au code UAI sélectionné.

2.6.2.3.3. Exemple

Un utilisateur accède à une ressource pour laquelle son établissement a souscrit un abonnement.

⁸ Afin de proposer un identifiant qui ne permette pas d'être associé à l'identité de l'accédant, la méthode proposée est la suivante.

Cet identifiant est de la forme «LxxCjjMmaahhmmsszzz» avec :

- L et C correspondent aux codes du porteur de projet de l'ENT (cf. chapitre 5.2 « Codes des projets ENT ») ;
- xx : 2 lettres à générer pour chaque entrée ;
- jjMmaahhmmsszzz : 15 chiffres à générer pour chaque entrée à partir de la date de création de l'identifiant opaque ou du compte utilisateur à la milliseconde avec :
 - jj : jour de création sur deux caractères ;
 - mm : mois de création sur deux caractères ;
 - aa : année de création sur deux caractères ;
 - hh : heure de création sur deux caractères ;
 - ss : seconde de création sur deux caractères ;
 - zzz : milliseconde de création sur trois caractères.

Seul le code UAI est nécessaire si tous les usagers de l'établissement ont les mêmes autorisations sur la ressource. S'il y a des autorisations différentes par profil (par exemple pour les enseignants ou les élèves), la solution ENT peut également transmettre le profil de l'accédant.

L'identifiant de l'utilisateur est nécessaire afin de lui proposer des services personnalisés.

2.6.2.4. Services de catégorie 4

Rappel : l'accès à un service de catégorie 4 s'effectue sur la base d'informations non nominatives transmises par l'ENT lors de la connexion et sur la base d'informations nominatives sur l'accédant, dont dispose au préalable le service Tiers (« mapping d'identités » réalisé par le service Tiers).

Le processus d'inscription au service applicatif s'effectue hors ENT.

2.6.2.4.1. Inscription d'un utilisateur

Les services Tiers appartenant à la catégorie 4 relèvent d'un processus d'inscription non corrélé à la connexion à un ENT. L'utilisateur s'inscrit au service Tiers et les moyens mis en œuvre pour effectuer cette inscription sont gérés par le service Tiers lui-même : inscription sur le site internet du service Tiers, inscription « papier », etc.

2.6.2.4.2. Cinématique fonctionnelle

L'accès au service via l'ENT nécessite d'établir le « mapping » entre l'utilisateur de l'ENT et le compte créé par le service Tiers lors de l'inscription de la personne. Ce « mapping » est réalisé lors de la première connexion de la personne au service via l'ENT (première connexion ou réabonnement, nouvelle année scolaire...). Le cas particulier de la première connexion est donc décrit ci-après de façon distincte de la connexion nominale.

Cas de la première connexion

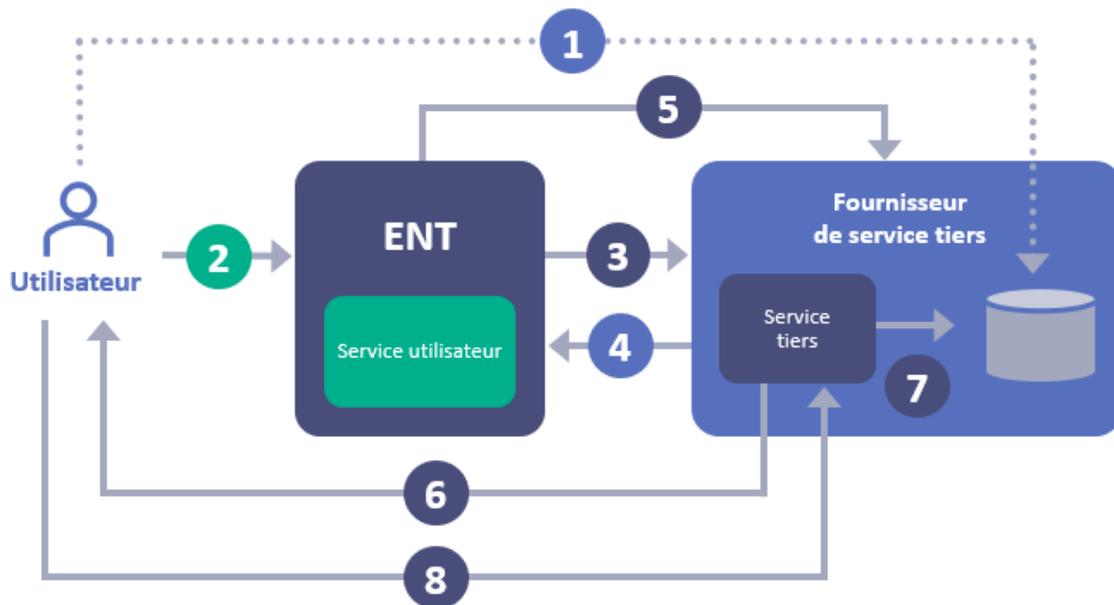


Figure 12 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la première connexion)

Comme illustré Figure 12, la cinématique d'accès à un service de la catégorie 4 est la suivante, pour la première connexion :

- 1) l'utilisateur s'est préalablement inscrit auprès du service via un processus hors ENT ;
- 2) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 3) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 4) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
- 5) la solution ENT transmet un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
- 6) à la première connexion, le service Tiers demande à l'utilisateur de s'authentifier à l'aide des informations d'authentification reçues lors de l'inscription préalable ;
- 7) le service Tiers réalise et stocke le lien entre l'identifiant fourni par l'utilisateur et celui transmis par l'ENT (« mapping » d'identités) ;
- 8) l'utilisateur accède de façon nominative au service Tiers.

Cas de la connexion nominale

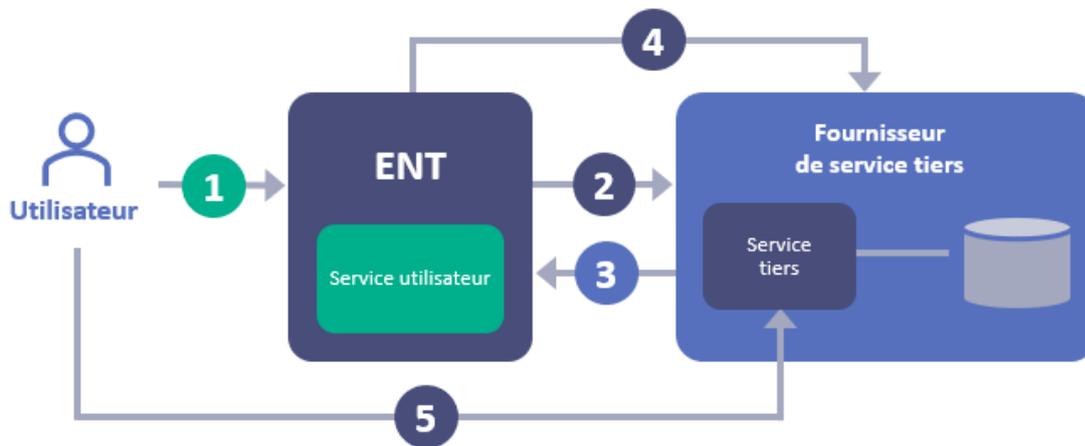


Figure 13 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la connexion nominale)

Comme illustré Figure 13, la cinématique d'accès à un service de la catégorie 4 est la suivante, dans le cas de la connexion nominale :

- 1) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
- 4) la solution ENT transmet un **identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure** (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
- 5) l'identifiant transmis par l'ENT est reconnu par le service Tiers, l'utilisateur accède au service sans s'authentifier à nouveau.

2.6.2.4.3. Données transmises

Lors de l'inscription préalable hors ENT, le service Tiers **PEUT** demander à l'utilisateur des attributs afin de réaliser, par la suite, l'authentification, le contrôle d'accès ou la personnalisation. Par ailleurs, à cette occasion, le service Tiers **DOIT** faire mention des conditions générales d'accès au service dans le respect des conditions définies dans le registre des traitements pour le traitement en question.

Les données qui **PEUVENT** être transmises par la solution ENT afin d'assurer l'authentification et le contrôle d'accès sont :

- un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant⁹ ;
- l'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. chapitre 5.2 « Codes des projets ENT ») ;
- l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ;

Toute autre donnée **NE DOIT PAS** être transmise.

2.6.2.4.4. Exemple

Un utilisateur s'inscrit directement sur le site d'un fournisseur de ressources. Il fournit à ce dernier les informations permettant de créer un compte.

La première fois que l'utilisateur souhaite accéder à sa ressource via l'ENT, l'identifiant de l'utilisateur est transmis au fournisseur de service, et celui-ci demande à l'utilisateur de s'authentifier. Une fois l'utilisateur authentifié, le fournisseur de service met en correspondance l'identifiant de l'utilisateur avec le compte de ce dernier afin que celui-ci n'ait plus à s'authentifier lors des prochains accès.

2.6.2.5. Services de catégorie 5

Rappel : l'accès au service s'effectue sur la base d'informations fournies par l'utilisateur lors de la première connexion au service Tiers via l'ENT (formulaire en ligne...).

Lors des connexions suivantes, l'accédant sera reconnu par le service Tiers sur la base d'informations utilisateur transmises par l'ENT (fonctionnement identique à la catégorie 4 : mapping d'identités).

2.6.2.5.1. Inscription d'un utilisateur

Pour les services Tiers appartenant à la catégorie 5, l'inscription s'effectue dynamiquement lors de la « première connexion » de l'utilisateur au service via l'ENT (première connexion ou réabonnement, nouvelle année scolaire...). À la différence de la catégorie 4, le processus d'inscription au service Tiers est corrélé à la connexion à un ENT.

Le cas particulier de la première connexion est donc décrit ci-après de façon distincte de la connexion nominale.

⁹ Afin de proposer un identifiant qui ne permette pas d'être associé à l'identité de l'accédant, la méthode proposée est la suivante.

Cet identifiant est de la forme «LxxCjjMMaahhmmsszzz» avec :

- L et C correspondent aux codes du porteur de projet de l'ENT (cf. chapitre 5.2 « Codes des projets ENT ») ;
- xx : 2 lettres à générer pour chaque entrée ;
- jjMMaahhmmsszzz : 15 chiffres à générer pour chaque entrée à partir de la date de création de l'identifiant opaque ou du compte utilisateur à la milliseconde avec :
 - jj : jour de création sur deux caractères ;
 - MM : mois de création sur deux caractères ;
 - aa : année de création sur deux caractères ;
 - hh : heure de création sur deux caractères ;
 - ss : seconde de création sur deux caractères ;
 - zzz : milliseconde de création sur trois caractères.

En conséquence, il est important pour les porteurs de projet et les responsables de traitement de s'assurer que les données définies dans le cadre de la convention de service comme pouvant être transmises via l'ENT, correspondent bien aux finalités du service Tiers. De plus, les utilisateurs doivent être acteurs dans la validation des données transmises qui les concernent.

2.6.2.5.2. Cinématique fonctionnelle

Cas de la première connexion

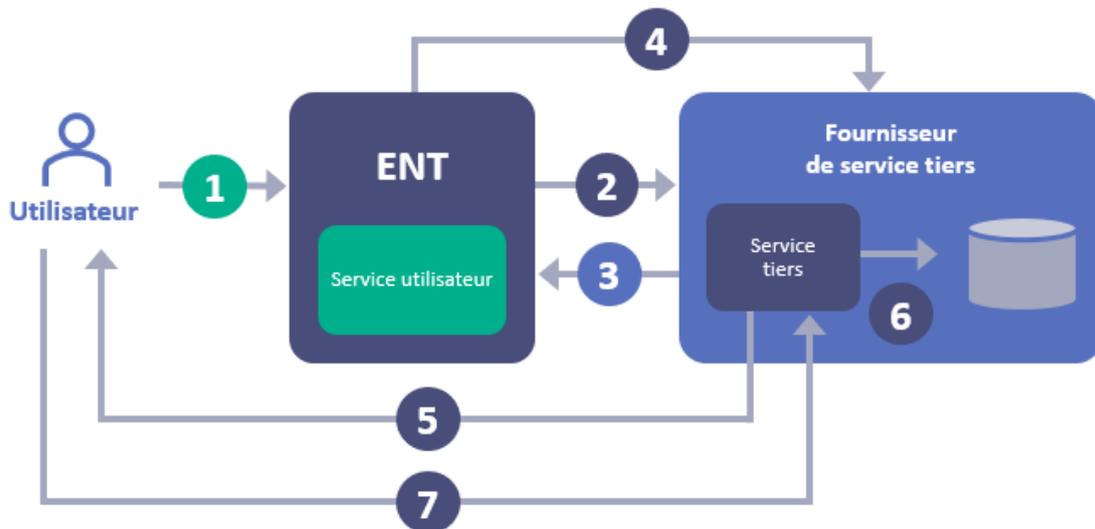


Figure 14 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la première connexion)

Comme le représente la Figure 14, la cinématique d'accès à un service de la catégorie 5 est la suivante pour la première connexion :

- 1) l'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
- 4) la solution ENT transmet un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
- 5) à la première connexion, l'utilisateur n'est pas reconnu par le service applicatif Tiers ; le service Tiers demande alors à l'utilisateur de remplir un formulaire d'inscription ;
- 6) le service Tiers stocke les informations transmises par l'utilisateur ;
- 7) l'utilisateur accède de façon nominative au service Tiers.

Cas de la connexion nominale

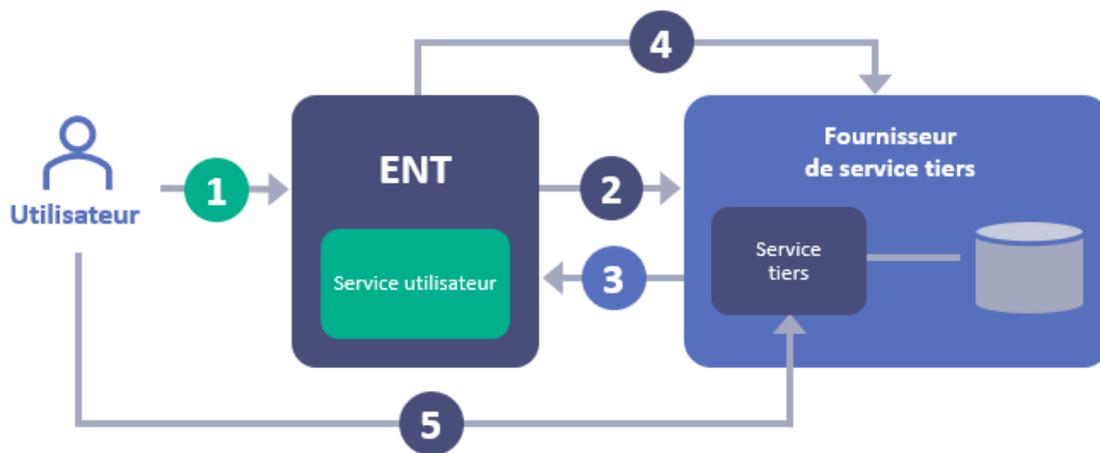


Figure 15 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la connexion nominale)

Comme le représente la Figure 15, la cinématique d'accès à un service de la catégorie 5 est la suivante, dans le cas d'une connexion nominale :

- 1) l'utilisateur s'authentifie à son ENT ou auprès d'un fournisseur d'identité externe via son login et son mot de passe ;
- 2) l'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
- 3) le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
- 4) la solution ENT transmet **un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure** (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
- 5) l'identifiant fourni par la solution ENT est reconnu par le service, l'utilisateur accède au service **sans s'authentifier à nouveau**.

2.6.2.5.3. Données transmises

Les informations d'identité qui peuvent être demandées à l'utilisateur lors de la première connexion **DOIVENT** être déclarées préalablement dans la convention de service.

Les informations d'identité **NE DOIVENT PAS** être transmises au service Tiers de façon automatique par l'ENT : l'ENT doit présenter à l'utilisateur la liste complète des informations d'identité demandées par le service Tiers et **DOIT** demander à l'utilisateur son consentement.

L'utilisateur **DOIT** avoir le choix de transmettre ou non ses informations d'identité.

Les informations d'identité **DOIVENT** être demandées au détail et dans la limite du nécessaire par rapport à la finalité du service Tiers (authentification, contrôle d'accès, personnalisation, suivi de l'utilisateur).

Remarque : toutes les informations transmises lors de cette première connexion sont fournies sur la base du volontariat de l'accédant. À cette occasion, les conditions générales d'accès au service **DEVRONT** y être explicitement précisées.

2.6.2.5.4. Exemple

Un utilisateur souhaite accéder via l'ENT à des ressources proposées par un fournisseur chez lequel il n'a pas de compte.

La première fois que l'utilisateur souhaite accéder à sa ressource via l'ENT, l'identifiant de l'utilisateur est transmis au fournisseur de service, et celui-ci demande à l'utilisateur de créer un compte. Les informations nécessaires à la création du compte sont donc transmises, et une fois le compte créé, le fournisseur de service met en correspondance l'identifiant de l'utilisateur avec le compte de ce dernier afin que celui-ci n'ait pas à créer de compte ni à s'authentifier lors des prochains accès.

2.6.3. Conventions de service

2.6.3.1. Généralités

Lorsque les acteurs du projet ENT (académie-collectivités, ou écoles / établissements scolaires) souhaitent interfacier l'ENT avec un service Tiers, une convention de service **DOIT** être élaborée entre les parties concernées, comme avait pu le préconiser la CNIL (délibération n°2006 – 104 du 27 avril 2007 relative aux ENT), afin que les rôles respectifs au sein de ces projets, leurs engagements et le traitement des données à caractère personnel des utilisateurs soient précisément définis.

Les points à traiter de ladite convention sont détaillés au chapitre 2.6.3.2. Notons que cette partie ne traite pas d'une manière exhaustive l'ensemble des points qui pourraient être évoqués à l'occasion de tels projets, mais liste les éléments indispensables pour qu'un service Tiers puisse s'interfacier avec un ENT.

La convention de service peut être apparentée à un sous-ensemble d'un accord de fédération entre un fournisseur d'identité et un fournisseur de service. Elle ne décrit cependant pas les engagements communs, tels que la mise en œuvre de standards technologiques.

2.6.3.2. Éléments à traiter

Ce chapitre précise les éléments à traiter dans la convention de service lors de la mise en œuvre d'un projet ENT.

2.6.3.2.1. Identification des parties concernées

La convention de service **DOIT** comporter

- la liste des parties concernées, par exemple :
 - ▶ le responsable de traitement de l'ENT (chef d'établissement, IA-DASEN), dans le cas de transmission de données à caractère personnel ;
 - ▶ le(s) responsable(s) de la mise en œuvre du projet ENT (collectivités, services académiques),
 - ▶ le responsable du service Tiers ;
- ainsi que le rôle de chacun :
 - ▶ responsable de traitement,
 - ▶ fournisseur d'identité,
 - ▶ fournisseur de service.

2.6.3.2.2. Organisation

L'organisation entre les différentes parties **DOIT** être précisée dans la convention de service.

En particulier, elle fera apparaître :

- les moyens mis en œuvre pour assurer la coordination entre les différentes parties ;
- les conditions d'adhésion et de retrait du responsable de la mise en œuvre du projet ENT ;
- les conditions d'adhésion et de retrait du responsable du service Tiers ;
- les relations entre membres : définition des relations bilatérales acceptées entre un fournisseur de service et un fournisseur d'identité ;
- la définition des documents de référence (dont les documents d'architecture technique).

2.6.3.2.3. Engagements respectifs des acteurs

La convention de service **DOIT** préciser les engagements des différents acteurs, à savoir :

- les responsabilités communes ;
- les engagements des fournisseurs d'identité (cf. chapitre 2.2.5) ;
- les engagements des fournisseurs de service (cf. chapitre 2.2.5) ;
- les engagements des administrateurs de la solution ENT ;
- la durée de l'accord et les conditions de rupture et de renouvellement.

2.6.3.2.4. Conditions et modalités d'accès / retrait au service Tiers

La convention de service **DOIT** faire apparaître notamment les conditions (qualité de service par exemple) et modalités d'accès et de retrait d'un utilisateur à un service Tiers, notamment, celle-ci mentionnera les éléments suivants :

- accès / retrait d'un utilisateur de **sa propre initiative** (via l'ENT, via un formulaire en ligne à la première connexion...);
- accès / retrait d'un utilisateur **par un tiers** (directeur d'école, chef d'établissement, administrateur de l'ENT...);
- durée de conservation, récupération et suppression des données à caractère personnel dont les données produites dans les services Tiers.

2.6.3.2.5. Données transmises

La convention de service **DOIT** stipuler clairement les données nécessaires devant être transmises par l'ENT afin d'assurer l'authentification et le contrôle d'accès et indispensables au fonctionnement du service Tiers ainsi que les destinataires et la finalité du traitement de données à caractère personnel le cas échéant, en respectant les données autorisées selon la catégorie du services Tiers définies plus haut et les dispositions légales et réglementaires en vigueur.

Les données transmises ne peuvent pas être utilisées à d'autres finalités de traitement que celles indispensables à la fourniture du service.

2.6.3.2.6. Capacité à sous-traiter

La convention de service **DOIT** préciser la capacité d'un des acteurs du projet à sous-traiter tout ou partie de ses activités. Le cas échéant, les conditions, devoirs et responsabilités relatifs à cette sous-traitance **DOIVENT** être précisés dans la convention.

2.6.3.2.7. Autres points à traiter

Les parties concernées sont libres de faire apparaître dans la convention de service tous les éléments complémentaires qui leur semblent importants de souligner dans le cadre du projet ENT, sous réserve que ces éléments respectent la législation en vigueur, et soient notamment conformes aux informations visées dans le registre des traitements pour le traitement en question.

2.6.4. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Sécurité interfaçage service Tiers (SSO sans fédération d'identités)	Les échanges de données autorisés dans le cadre d'un interfaçage de l'ENT avec un service Tiers DOIVENT respecter les règles associées à la catégorie du service tel que présentées au chapitre « Exigences et recommandations pour l'interfaçage entre l'ENT et les services Tiers » de l'annexe opérationnelle.	E	E
02	Sécurité interfaçage service Tiers de catégorie 1	La solution ENT NE DOIT PAS transmettre d'information d'identité sur l'utilisateur à un service Tiers de catégorie 1.	E	E
03	Sécurité interfaçage service Tiers de catégorie 2	<p>Les données que la solution ENT est autorisée à transmettre à un service Tiers de catégorie 2 afin d'assurer l'authentification et le contrôle d'accès sont :</p> <ul style="list-style-type: none"> ▪ l'identifiant du projet ENT à partir duquel le service Tiers est appelé (code projet ENT tel que défini dans l'annexe opérationnelle) ; ▪ l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ; ▪ le profil de l'accédant, non associé à une identité (tel que défini dans l'annexe opérationnelle). <p>La solution ENT est autorisée à transmettre à un service Tiers de catégorie 2 d'autres attributs non associés à une identité ; la liste de ces attributs est donnée au chapitre « Recommandations pour l'interfaçage entre l'ENT et les services Tiers / Services de catégorie 2 » de l'annexe opérationnelle.</p> <p>La solution ENT NE DOIT PAS transmettre d'autre donnée à un service Tiers de catégorie 2.</p>	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
04	Sécurité interfaçage service Tiers de catégorie 3	<p>Les données que la solution ENT est autorisée à transmettre à un service Tiers de catégorie 3 afin d'assurer l'authentification et le contrôle d'accès sont :</p> <ul style="list-style-type: none"> ▪ un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant (tel que défini dans l'annexe opérationnelle) ; ▪ l'identifiant du projet ENT à partir duquel le service Tiers est appelé (code projet ENT tel que défini dans l'annexe opérationnelle) ; ▪ l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ; ▪ le profil de l'accédant, non associé à une identité (tel que défini dans l'annexe opérationnelle). <p>La solution ENT est autorisée à transmettre à un service Tiers de catégorie 3 d'autres attributs non associés à une identité ; la liste de ces attributs est donnée dans au chapitre « Recommandations pour l'interfaçage entre l'ENT et les services Tiers / Services de catégorie 3 » de l'annexe opérationnelle.</p> <p>La solution ENT NE DOIT PAS transmettre d'autre donnée à un service Tiers de catégorie 3.</p>	E	E
05	Inscription préalable à un service Tiers de catégorie 4	<p>Lors de l'inscription préalable d'un utilisateur à ses services (process hors ENT), où l'utilisateur s'inscrit, le service Tiers peut demander à l'utilisateur des attributs afin de réaliser, par la suite, l'authentification, le contrôle d'accès ou la personnalisation.</p> <p>À cette occasion, le service Tiers DOIT faire mention des conditions générales d'accès au service dans le respect des conditions définies dans le registre des traitements pour le traitement en question.</p>	E	E
06	Sécurité interfaçage service Tiers de catégorie 4	<p>Les données que la solution ENT est autorisée à transmettre à un service Tiers de catégorie 4 afin d'assurer l'authentification et le contrôle d'accès sont :</p> <ul style="list-style-type: none"> ▪ un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant (tel que défini dans l'annexe opérationnelle) ; ▪ l'identifiant du projet ENT à partir duquel le service Tiers est appelé (code projet ENT tel que défini dans l'annexe opérationnelle) ; ▪ l'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ; <p>La solution ENT NE DOIT PAS transmettre d'autre donnée à un service Tiers de catégorie 4.</p>	E	E
07	Sécurité interfaçage service Tiers de catégorie 5	<p>Les informations d'identité qui peuvent être demandées à l'utilisateur lors de la première connexion, DOIVENT être déclarées préalablement dans la convention de service.</p> <p>Les informations d'identité DOIVENT être demandées au détail et dans la limite du nécessaire par rapport à la finalité du service Tiers (authentification, contrôle d'accès, personnalisation, suivi de l'utilisateur).</p>	E	E
08	Sécurité interfaçage service Tiers de catégorie 5	<p>Lors de la première connexion de l'utilisateur, lorsqu'il lui est demandé de fournir les informations le concernant, les conditions générales d'accès au service Tiers DOIVENT être explicitement précisées et conformes aux informations visées dans le registre des traitements pour le traitement en question.</p>	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
09	Sécurité interfaçage service Tiers de catégorie 5	Les informations d'identité NE DOIVENT PAS être transmises au service Tiers de façon automatique par l'ENT : l'ENT doit présenter à l'utilisateur la liste complète des informations d'identité demandées par le service Tiers et DOIT demander à l'utilisateur son consentement. L'utilisateur DOIT avoir le choix de transmettre ou non ses informations d'identité.	E	E
10	Convention de service	Concernant l'interopérabilité de la solution ENT avec des services Tiers, une convention de service DOIT être élaborée afin que les rôles respectifs, les engagements et les modalités de traitement des données à caractère personnel des acteurs soient précisément définis.	E	E
11	Convention de service	La convention de service DOIT comporter la liste des parties concernées, par exemple : <ul style="list-style-type: none"> ▪ le responsable de traitement de l'ENT (chef d'établissement, IA-DASEN) dans le cas de transmission de données à caractère personnel ; ▪ le(s) responsable(s) de la mise en œuvre du projet ENT (collectivités, services académiques) ; ▪ le responsable du service Tiers. La convention de service DOIT comporter le rôle de chacun : <ul style="list-style-type: none"> ▪ responsable de traitement ; ▪ fournisseur d'identité ; ▪ fournisseur de service. 	E	E
12	Convention de service	L'organisation entre les différentes parties DOIT être précisée dans la convention de service. En particulier, elle fera apparaître : <ul style="list-style-type: none"> ▪ les moyens mis en œuvre pour assurer la coordination entre les différentes parties ; ▪ les conditions d'adhésion et de retrait du fournisseur d'identité ; ▪ les conditions d'adhésion et de retrait du responsable du service Tiers ; ▪ les relations entre membres : définition des relations bilatérales acceptées entre un fournisseur de service et un fournisseur d'identité ; ▪ la définition des documents de référence (dont les documents d'architecture technique). 	E	E
13	Convention de service	La convention de service DOIT préciser les engagements des différents acteurs, à savoir : <ul style="list-style-type: none"> ▪ les responsabilités communes ; ▪ les engagements des fournisseurs d'identité ; ▪ les engagements des fournisseurs de service ; ▪ les engagements des administrateurs de la solution ENT ; ▪ la durée de l'accord et les conditions de rupture et de renouvellement. 	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
14	Convention de service	<p>La convention de service DOIT faire apparaître les conditions (qualité de service par exemple) et modalités d'accès et de retrait d'un utilisateur à un service Tiers, notamment, celle-ci mentionnera les éléments suivants :</p> <ul style="list-style-type: none"> ▪ accès / retrait d'un utilisateur de sa propre initiative (via l'ENT, via un formulaire en ligne à la première connexion...); ▪ accès / retrait d'un utilisateur par un tiers (directeur d'école, chef d'établissement, administrateur de l'ENT...); ▪ durée de conservation, récupération et suppression des données à caractère personnel dont les données produites dans les services Tiers. 	E	E
15	Convention de service	<p>La convention de service DOIT stipuler clairement les données nécessaires devant être transmises afin d'assurer l'authentification et le contrôle d'accès et indispensables au fonctionnement du service Tiers ainsi que les destinataires et la finalité du traitement de données à caractère personnel le cas échéant en respectant les données autorisées selon la catégorie du service Tiers définies dans l'annexe opérationnelle et les dispositions légales et réglementaires en vigueur.</p>	E	E
16	Convention de service	<p>La convention de service DOIT préciser la capacité d'un des acteurs du projet à sous-traiter tout ou partie de ses activités. Le cas échéant, les conditions, devoirs et responsabilités relatifs à cette sous-traitance DOIVENT être précisés dans la convention.</p>	E	E

Tableau 7 : Exigences et recommandations concernant l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités

3. Méthodes d'intégration

3.1. Introduction

Ce paragraphe détaille uniquement la méthode d'Api-sation des ENT. Il sera susceptible dans les prochaines versions d'aborder d'autres méthodes d'intégration.

Ce chapitre de l'annexe opérationnelle du SDET s'inscrit dans le cadre des qualités attendues d'un ENT au titre de l'interopérabilité, particulièrement celles de permettre l'interopérabilité des systèmes et les interactions avec les différents services / applications.

Il complète la description de quatre des services du domaine **services Socle Intégration** de l'architecture de référence regroupés ici sous la dénomination **services INT** ; en l'occurrence :

- Import / export de données [SOC-INT-IED] ;
- Appel de services externes [SOC-INT-ASE] ;
- Présentation de services vers l'extérieur [SOC-INT-PSE]
- Mise à disposition des données aux services [SOC-INT-MDD].

À cet effet, il fournit un ensemble de définitions destinées à préciser certains concepts et des exigences et des recommandations à respecter afin que tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire évoluent dans un cadre de confiance autour de l'interfaçage entre l'ENT et les services externes au projet ENT (services Tiers)

3.2. Interface applicative de Programmation (API)

3.2.1. Présentation

Les API (*Application Programming Interface*) permettent l'intégration, c'est-à-dire la connexion de données, d'applications et de périphériques au sein de services informatiques pour que l'ensemble des technologies puissent communiquer et interagir plus efficacement ou permettent de rendre disponibles des données ou des fonctionnalités d'application existante à d'autres applications externes.

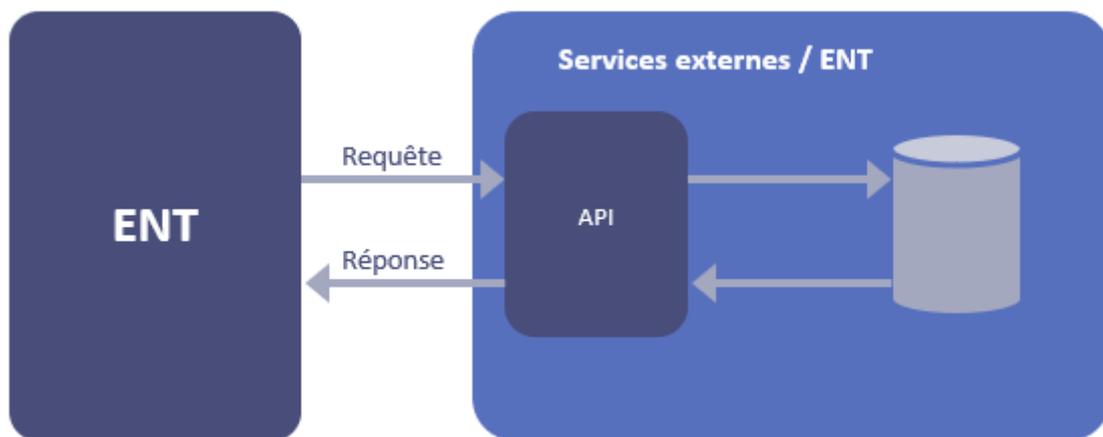


Figure 16 : Echanges entre l'ENT et les services externes de l'ENT via API

3.2.2. APIisation de l'ENT

De plus en plus de services exposent des API qui permet à un client (un ENT, un autre service) d'interagir avec une autre application. Afin de proposer une API à d'autres services, il est important de prendre en compte deux éléments dans la construction de l'API :

- S'assurer que l'API puisse être appelée quel que soit le client / la plateforme utilisé(e). Cela requiert l'utilisation de protocoles standard et une définition du format des données à échanger
- L'API et ses fonctionnalités doivent pouvoir évoluer indépendamment des applications clientes. Au fur et à mesure que l'API évolue, les applications clientes existantes doivent pouvoir continuer de fonctionner sans modifications.

L'ensemble des fonctionnalités disponibles peuvent être appelées par d'autres applications via Internet avec différents types API dites API Webservices. Ces API s'adossent sur deux grands protocoles de communication : : Simple Object Access Protocol (SOAP) et Representational State Transfer (REST).

Le protocole SOAP permet de structurer fortement les échanges entre applications mais a comme gros inconvénient le poids des flux échangés et un XML est très verbeux.

L'architecture REST, plus simple, moins structurée mais beaucoup plus léger, basée sur le JSON, et qui peut également retourner d'autres formats : JSON, XML, HTML, CSV... Autre point important, le JSON (JavaScript Object Notation) offre l'énorme avantage d'être directement interprété par le javascript, langage devenu universel avec la fin de vie de Flash.

Les API REST sont conçues autour de ressources (identifiable avec un identificateur URI qui identifie de façon unique cette ressource), qui peuvent être tout type de données, d'objets, de service accessibles par le client. Pour les API REST qui reposent sur HTTP, l'utilisation de verbes HTTP standard (GET, POST, PUT et DELETE) est utiliser pour effectuer des opérations sur les ressources (récupération de données, mise à jour de données, ajout de données, suppressions de données).

Une autre alternative complémentaire aux API REST : GraphQL qui est un langage de requête pour les API et qui propose une approche totalement différente des API REST car il permet de centraliser les requêtes dans un seul point d'entrée.

L'avantage principal est que le client (le navigateur) décrit la réponse qu'il souhaite recevoir. Cela évite au serveur de retourner trop d'information.

Le principal inconvénient de GraphQL est la gestion du cache (pas de mutualisation du cache possible, les requêtes étant spécifiques).

3.2.3. Exposition de données et des services

L'exposition des données par une API permet la mise à disposition de contenus d'un système d'information grâce à des URI, dans un format de données structurées. La protection de la donnée devient très vite primordiale dans l'ouverture des données vers un écosystème extérieur. La démarche « d'APIsation » doit garantir également la mise en place de bonnes pratiques en termes de sécurité de la donnée. Ce type d'architecture est généralement associé avec la mise en place de cadres réglementaires comme le RGPD.

Les quatre verbes HTTP principaux pris en charge par les API REST incluent :

- GET : utilisé pour demander des données à un serveur (par exemple, récupérer les données client), rappelle l'opération **Read** ou **Retrieve** dans le terme **CRUD** étroitement lié avec la gestion des bases de données.
- POST : utilisé pour envoyer des données d'un client au serveur (par exemple pour ajouter un nouveau client), rappelle l'opération **Create** dans le terme **CRUD**.
- PUT : utilisé pour mettre à jour les informations existantes sur le serveur, rappelle l'opération **Update** dans le terme **CRUD**.
- DELETE : Utilisé pour supprimer des informations sur le serveur, rappelle l'opération **Delete** dans le terme **CRUD**.

En plus d'exposer des données, une API peut également exposer des services, des fonctionnalités comme un ensemble de ressources identifiables par un URI et accessibles par la syntaxe et la sémantique du protocole HTTP.

3.2.4. Versionning des API

Une API est vouée à évoluer en fonction de l'enrichissement du modèle de données mais aussi des besoins du service qui consomme cette API. Cette évolution de l'API peut avoir des impacts sur les applications clientes utilisant l'API. Il est donc indispensable de versionner les API afin de limiter les impacts dans le cas où certaines applications continueraient à utiliser la première version de l'API et de nouvelles applications utiliseraient la nouvelle version enrichie de l'API.

Le contrôle de version permet à une API web d'indiquer les fonctionnalités et ressources qu'elle expose. Une application cliente peut alors envoyer des requêtes destinées à une version spécifique d'une fonctionnalité ou d'une ressource.

L'approche la plus courante pour le versionning des API est le contrôle de version d'URI. Ainsi les applications déjà consommatrices de l'API web continueront à fonctionner sans impact et les nouvelles applications auront le nouvel URI (lien qui pointera vers la version de la ressource) pour consulter les données.

D'autres approches existent :

- Contrôle de version de chaîne de requête (la version est ajoutée dans la requête http)
- Contrôle de version d'en-tête (en-tête personnalisé qui indique la version de la ressource)

3.2.5. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1 ^{er} degré 1D	Préconisation 2 nd degré 2D
01	API	Afin de limiter la taille des messages échangés entre les systèmes, le système mettant à disposition une API DOIT proposer une API compatible REST	E	E
02	API	Le système mettant à disposition des API REST DOIT limiter les opérations en termes de méthodes http aux opérations GET ou POST. En effet il NE DOIT PAS être possible pour un système A de mettre à jour (PUT) ou supprimer (DELETE) des données d'un système B.	E	E
03	API	Afin de respecter la confidentialité des données qui transitent et leur traitement, il DOIT être utilisé des mécanismes d'authentification (par exemple oAuth2) et d'autorisation forte (par exemple OpenID Connect) qui vont permettre de contrôler strictement l'accès aux systèmes et aux données.	E	E
04	API	Le système mettant à disposition des API DOIT gérer le contrôle de version des API afin de permettre de garantir la compatibilité descendante d'un service tout en ajoutant de nouvelles fonctionnalités ou en mettant à jour les fonctionnalités existantes pour les nouveaux clients	E	E
05	API	Les API NE DOIVENT PAS renvoyer plus d'informations que nécessaire pour remplir leur fonction	E	E

4. Stratégie d'exploitation

4.1. Introduction

Ce chapitre apporte des préconisations sur l'organisation de l'exploitation des ENT.

Il complète le document principal sur les aspects de mise en œuvre, et notamment :

- la description des services « Exploitation », « Hébergement », et « Administration et back office » du domaine « Services Support » des Services Socle ;
- les qualités de performance et de disponibilité attendues d'un ENT au titre de la qualité de l'expérience utilisateur.

À cet effet, il fournit un ensemble de recommandations pour les processus des différentes phases des projets qu'il faudra décliner pour l'ensemble des acteurs et intégrer dans la contractualisation de ces acteurs.

Ces recommandations couvrent deux aspects :

- certaines recommandations définissent des règles ou des principes à respecter ;
- d'autres indiquent des travaux complémentaires à mener sur lesquels chaque acteur de projet ENT doit se positionner.

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

Ce chapitre complète le document principal sur le thème de la stratégie d'exploitation en précisant les trois sujets d'attention suivants, qui donnent lieu chacun à un chapitre :

- les prestataires et la contractualisation ;
- les moyens de qualifier la solution ENT ;
- la fourniture de l'ENT et ses évolutions.

4.2. Les prestataires et la contractualisation

Avant même de définir les conditions d'exploitation propres à satisfaire les besoins des utilisateurs, ces besoins doivent être explicités sous forme d'exigences de qualité de service déclinées pour chacun des acteurs et contractants selon leur domaine de responsabilité.

C'est le but des **conventions de service** qui permettent de mettre au point, entre les utilisateurs et les responsables des différents domaines de responsabilité, les attentes des premiers et les engagements des seconds.

4.2.1. Principes généraux

Les objectifs de qualité de service **DOIVENT** être déclinés sous forme d'engagements personnalisés fixés à chacun des acteurs et contractants en fonction de leur domaine de responsabilité, de sorte que le respect de ces différents engagements permette d'atteindre le niveau de qualité de service global fixé pour l'ENT.

Le respect de ces engagements **DOIT** être contrôlé.

La définition de ces engagements et l'effectivité des contrôles peuvent être complexes si les contractants sont nombreux ou si les tâches et responsabilités n'ont pas été réparties de manière simple. Il sera par exemple difficile de déterminer la responsabilité d'un acteur dans le cas de dégradation de la disponibilité ou des performances si les composants des services applicatifs et des services Socle ont été répartis dans les domaines de plusieurs prestataires externes. Il sera également, dans ce cas, plus difficile de synchroniser les tâches de ces différents acteurs lors d'évolutions de l'ENT ou du traitement de résolutions d'incidents complexes. Par ailleurs, les organisations, les besoins, les fonctions et les technologies sont amenés à évoluer tout au long du cycle de vie de l'ENT. La flexibilité sera d'autant plus importante qu'il n'y aura pas un niveau d'interdépendance élevé entre les contrats de plusieurs partenaires, leurs moyens techniques et leurs processus.

Le porteur de projet **DEVRAIT** limiter le nombre de contrats passés avec des prestataires extérieurs, à charge pour ces derniers de sous-traiter des tâches spécifiques à d'éventuels partenaires.

La mise en œuvre du projet ENT peut par exemple être organisée avec un intégrateur global au niveau du projet ENT, un « mainteneur » unique responsable des logiciels applicatifs de la solution ENT, et un hébergeur/exploitant unique responsable du service opérationnel de la solution ENT.

4.2.2. Relations entre intégrateur et mainteneur

Ce chapitre traite du choix d'acteurs différents ou non pour la mise en place de la solution ENT (« intégrateur / éditeur initial »), et pour sa maintenance (« mainteneur »)¹⁰.

Les activités d'intégration/édition et de maintenance requièrent des compétences communes ; aussi, l'intégrateur/éditeur initial est souvent retenu pour la maintenance de la solution ENT. Afin de limiter le risque d'une trop grande dépendance avec le prestataire, il est nécessaire de prévoir :

- une clause de réversibilité afin de permettre un éventuel transfert de responsabilités vers un nouvel acteur dans le cas d'une résiliation ou d'un non renouvellement du contrat ; cette clause est de toute façon nécessaire pour le cas d'un changement de solution ENT ;
- une obligation du prestataire de maintenir à jour les différentes documentations (techniques ou relatives aux processus), au fil des évolutions ;
- des contrôles qui peuvent par exemple s'effectuer au travers de procédures d'audits de la qualité et de la maintenabilité des développements spécifiques, ou au travers de la vérification de la complétude et de l'exactitude des documentations.

¹⁰ Cf. chapitre « Écosystème de l'ENT » du document principal

Bien que cela nécessite un effort de transfert de compétences et de responsabilités, la possibilité de contractualisation avec un mainteneur différent de l'intégrateur d'origine est à considérer. Elle est le signe d'une solution ENT mature présentant un bon niveau de maintenabilité, permettant de se prévenir de la dépendance vis-à-vis d'acteurs spécifiques. Il est toutefois recommandé de ne pas effectuer ce changement dès la mise en service de la première version de la solution ENT ou d'une des évolutions majeures. Une attention particulière doit également être portée au transfert de responsabilités vers le nouveau mainteneur, celui-ci devant s'approprier le contexte sans dégradation du degré d'engagement sur le niveau de qualité de service.

En résumé :

- une clause de réversibilité et une obligation de mise à disposition des documentations actualisées **DOIVENT** être prévues au contrat avec l'intégrateur/éditeur initial ;
- la maintenance **PEUT** être confiée à un acteur différent de l'intégrateur/éditeur initial lorsque la mise en œuvre de la solution ENT est stabilisée.

4.2.3. Relations entre hébergeur/exploitant et intégrateur/éditeur/mainteneur

Ce chapitre aborde les interactions entre le responsable de la partie logicielle applicative de la solution ENT (le mainteneur, en relation avec l'intégrateur/éditeur, appelé ici « intégrateur/éditeur/mainteneur » ou par simplification « mainteneur »), et le responsable de sa mise en œuvre opérationnelle (l'exploitant, en relation avec l'hébergeur, appelé ici « hébergeur/exploitant » ou simplement « exploitant »).

Afin de simplifier la définition des domaines de responsabilité des différents prestataires, toutes les activités d'exploitation **PEUVENT** être confiées à l'hébergeur/exploitant, y compris toutes celles relatives à l'exploitation des services applicatifs (ex : maintenance des bases de données...).

Toutefois, les domaines de responsabilité entre hébergeur/exploitant et intégrateur/éditeur/mainteneur ne sont pas toujours simples à formaliser, et encore moins à décliner en indicateurs de mesure contractuels relatifs à la disponibilité et aux performances de la solution ENT.

Par exemple, après un incident ayant pour conséquence une rupture de service, l'hébergeur/exploitant est responsable de la remise en ordre de marche du service. Il est toutefois dans l'impossibilité de le faire si cette remise en service nécessite une action correctrice d'un logiciel, qui est dans le domaine de responsabilité du mainteneur. Dans ce cas, l'hébergeur/exploitant est tenu d'affecter l'incident, de transmettre les informations au mainteneur dans les plus brefs délais et de collaborer pour toute contribution d'analyse de la plateforme de production.

En ce qui concerne les performances, le partage de responsabilité peut s'avérer relativement complexe. Ainsi, la responsabilité d'une dégradation des performances due à une évolution de la charge ou du volume de données sera difficile à reporter sur un acteur si les ressources des serveurs et des réseaux ne sont pas saturées. L'amélioration d'une telle situation peut nécessiter des actions d'optimisation de services qui sont dans le domaine de responsabilité de l'hébergeur/exploitant (ex : défragmentation du disque, purge de données inutiles...) ou d'autres actions qui sont dans le domaine de responsabilité de l'intégrateur/éditeur/mainteneur (ex : optimisation des requêtes et des traitements des services applicatifs).

Ainsi, il peut arriver que les deux acteurs soient impliqués aussi bien dans l'analyse des causes de la dégradation des performances que dans la réalisation d'actions correctrices (palliatives et/ou définitives). Il est donc important de veiller à ce que les domaines de responsabilité dans le domaine des performances soient décrits avec précision dans les contrats de ces deux prestataires.

Pour ce faire, l'intégrateur/éditeur/mainteneur **DOIT** produire une étude de dimensionnement qui indique les conditions dans lesquelles il garantit la qualité de service demandée compte tenu de la volumétrie et des exigences du projet ENT, en particulier :

- les caractéristiques nécessaires de la plateforme (dimensionnement, paramétrage...);
- les actions particulières requises de l'hébergeur/exploitant – indicateurs applicatifs à surveiller, opérations récurrentes d'optimisation et de nettoyage, ordonnancement des traitements par lots...

Des campagnes de tests de performance **DEVRAIENT** être menées avant la mise en production de nouvelles versions applicatives afin d'anticiper un certain nombre de problèmes.

L'exploitation et la maintenance de l'ENT **PEUVENT** être confiées à un prestataire unique, si ses compétences le permettent, simplifiant ainsi les aspects contractuels. Dans ce cas, on préviendra le risque de perte de maîtrise et donc de dépendance par une attention particulière portée à la clause de réversibilité du contrat, par la possibilité de mener des actions de contrôle et d'audit et par une exigence de transparence minimale au niveau des activités effectuées et des coûts unitaires des devis.

En tout état de cause, tout prestataire **DOIT** être lié par un document contractuel. Celui-ci **DOIT** notamment contenir les obligations de sécurité et de confidentialité du sous-traitant conformément au RGPD et à la loi n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés modifiée.

4.2.4. Propriété des matériels et logiciels

4.2.4.1. Propriété du porteur de projet ENT

Les matériels et logiciels standards de base sont parfois la propriété du porteur de projet de l'ENT, qui signe alors les contrats de maintenance de ces composants. Les exploitants et mainteneurs de la solution ENT **DOIVENT**, dans ce cas, avoir accès au support prévu dans le cadre de ces contrats de maintenance.

4.2.4.2. Propriété du prestataire

Si les composants matériels et logiciels sont la propriété d'un prestataire, deux solutions se présentent :

- 1) le prestataire est engagé sur un niveau de qualité de service dans un contexte technique et fonctionnel et sur une volumétrie d'utilisation définis dans le contrat.
- 2) l'évolution des composants logiciels et matériels est à la charge du prestataire, qui a alors l'obligation d'effectuer toutes les opérations d'évolution garantissant le maintien d'un niveau de qualité de service élevé, quelle que soit l'évolution de la charge d'utilisation ou des contraintes techniques.

Concernant la **qualité de service** (cas 1), le prestataire **DOIT** alerter suffisamment à l'avance la maîtrise d'ouvrage du projet ENT de la nécessité de faire évoluer les composants logiciels et matériels pour maintenir une qualité de service élevée, notamment dans le cas d'évolutions

de la charge d'utilisation ou du volume de données, de l'usure des matériels et de la fin de vie (ou fin de support/maintenance) annoncée de logiciels ou matériels.

Ce prestataire **DOIT** de plus indiquer ses recommandations d'évolutions de la solution ENT tant au niveau des composants que de la démarche d'évolution (migration, déploiement...).

Concernant l'**évolution des composants logiciels et matériels** (cas 2), le mode de financement de ce prestataire **DOIT** dans ce cas être adapté en conséquence et, par exemple, être fonction de paramètres de volumétrie factuels (nombre d'utilisateurs déclarés ou simultanés, taille des données...). Les évolutions de la solution ENT doivent être effectuées en cohérence avec l'engagement de qualité de service contractualisé, à charge pour le prestataire de fiabiliser et d'optimiser les évolutions afin de minimiser les ruptures de service et les régressions liées à ces évolutions. Le prestataire doit être dans l'obligation d'informer l'équipe de maîtrise globale de la solution ENT, de manière anticipée, de toute évolution majeure planifiée et de tout risque lié aux évolutions.

En ce qui concerne les droits des développements spécifiques des services applicatifs réalisés par un prestataire extérieur :

- soit les droits patrimoniaux des développements spécifiques des services applicatifs sont transférés à la maîtrise d'ouvrage du projet ENT, à l'issue d'une phase de recette ;
- soit ces droits ne sont pas transférés (cas notamment des offres SaaS), et le contrat **DOIT**, dans ce cas, contenir une clause permettant d'assurer la pérennité de l'ENT en cas de défaillance du prestataire ou arrêt de maintenance des logiciels (dépôt des sources, accès aux sources...). Il est par ailleurs recommandé dans ce cas de s'assurer que la stratégie d'évolution de ces logiciels est compatible avec les contraintes et les besoins prévisibles du projet ENT.

4.2.5. Qualités des prestataires extérieurs et exigences contractuelles

La sélection des prestataires extérieurs s'attachera notamment à veiller qu'ils respectent les critères suivants :

- assurer une qualité de service optimum dans la durée ;
- être compétitif, aussi bien en ce qui concerne les prestations récurrentes ou prédéfinies dans le contrat, que les prestations à la demande ;
- être réactif face à une demande d'évolution des services ou de travaux d'exploitation ;
- être en mesure de s'adapter à des changements du contexte, de l'organisation, des processus ou du périmètre ;
- adopter une démarche d'amélioration constante de la qualité ;
- être en mesure de transférer l'activité à un tiers dans des conditions optimales.

Tout contrat avec un prestataire extérieur **DOIT** pouvoir être résilié pour manquement de l'une ou l'autre des parties ou pour non-respect chronique des niveaux de service contractualisés.

Le contrat **DOIT** exiger une garantie de bonne fin, en fin de marché ou après résiliation. Cette garantie **DOIT** inclure une clause de réversibilité permettant à un tiers de s'approprier l'activité dans des conditions optimales et sans risque de dégradation de la qualité de service ou de la maintenabilité de la solution ENT, en exigeant du prestataire initial sa participation

pour la migration éventuelle des services de l'ENT sur le nouveau site, et en assurant une continuité de service ou en limitant le temps d'indisponibilité lors du basculement.

Les domaines de responsabilité **DOIVENT** clairement être établis dans le contrat. Les objectifs de qualité de service **DOIVENT** être précisés, avec les indicateurs de mesure qui ne soient pas ambigus et auxquels est associée une méthode de mesure. Ces indicateurs donnent une vision simplifiée de la qualité de service.

Le contrat doit donc également contenir des garde-fous permettant de traiter des incidents de prestations ou de sécurité ayant pour conséquence ou pouvant entraîner un incident grave, et précisant un engagement sur un plan d'actions correctives ou préventives.

Un contrat doit engager le prestataire à respecter toutes les consignes de sécurité nécessaires et, notamment, sur les aspects de la confidentialité.

Qu'il s'agisse d'un prestataire de maintenance ou d'exploitation, celui-ci doit s'engager contractuellement sur des types de prestations prévisibles aussi bien en termes de coûts (unités d'œuvre) que de délais d'exécution, tout en maintenant l'engagement sur les niveaux de service fixés au départ. Cet engagement permet notamment d'obtenir une garantie de réactivité et de maintien des coûts.

Le fournisseur de l'ENT, ou intégrateur, doit, sur la base du cahier des charges, justifier les qualités de la solution qu'il propose en termes non seulement de conformité, de fiabilité, de performance et de sécurité, mais également d'évolutivité, de pérennité et de capacité à absorber les évolutions de charge et de volume de données.

4.3. Les moyens de qualifier la solution ENT

Toute mise en exploitation doit être précédée d'une série de tests et de travaux préalables à réaliser sur un équipement composé de plusieurs plateformes :

- une plateforme de développement utilisée pour le codage des développements spécifiques et la réalisation des tests unitaires ;
- une plateforme d'intégration et de recette, utilisée pour l'intégration des différents modules logiciels, la mise au point d'ensemble, la réalisation des tests fonctionnels et la recette avant la mise en production (Vérification d'aptitude au bon fonctionnement – VABF) ;
- une plateforme de diagnostic et de résolution d'incidents et de problèmes au même niveau applicatif que la plateforme de production ;
- une plateforme de préproduction, proche de la plateforme de production et dont la configuration est représentative de cette dernière, permettant de réaliser les tests de mise en production avant toute migration effective de la plateforme de production (Vérification d'aptitude à la bonne exploitabilité – VABE) ;
- la plateforme de production ;
- des plateformes de formation et de démonstration.

Par souci d'économies, il est recommandé d'étudier plusieurs scénarios possibles d'optimisation de ces moyens notamment lors de la consultation de soumissionnaires.

On utilise parfois, pour l'usage de diagnostic et de résolution d'incidents, la plateforme d'intégration, ou exceptionnellement celle de préproduction. Dans le premier cas, étant donné que sur la plateforme de diagnostic doivent être installées les versions des logiciels en production et sur celle d'intégration les versions des logiciels à mettre en exploitation (versions supérieures), le basculement d'une configuration à l'autre devra pouvoir se faire rapidement (ex : basculement de disques).

Les plateformes de formation et de démonstrations peuvent être distinctes. Il est possible de faire l'économie de ces plateformes en utilisant par exemple :

- la plateforme de production, pour des besoins de formation ou de démonstration de la version « courante » de la solution ENT (version en exploitation), sous réserve de précautions préalables notamment en termes de sécurité et de sûreté de fonctionnement : sécurité d'accès aux données sensibles, étanchéité des données réelles (données d'annuaire) et des données factices, suppression des données factices qui ne doivent pas apparaître dans les archives légales à la fin de la séance, non perturbation des performances... ;
- la plateforme d'intégration, pour la démonstration ou la formation sur une version de la solution ENT non encore déployée, sous réserve que les contraintes de planification soient compatibles et que les besoins prioritaires puissent être planifiés de manière fiable.

Dans le cas d'usages multiples de certaines plateformes, une gestion des priorités devra être mise en place afin de ne pas pénaliser la qualité de service.

De manière générale, les opérations de résolution des incidents majeurs en production doivent être prioritaires à toute autre activité - les plannings des autres projets devront être adaptés en conséquence.

Un cloisonnement de la plateforme de production **DOIT** être mis en place afin d'empêcher le moindre accès aux données de la solution ENT à partir d'une des autres plateformes.

On ne perdra pas de vue que les tests ne se limitent pas au fonctionnement de la solution ENT elle-même. En effet, celle-ci s'intègre dans un vaste ensemble de systèmes qui constituent une chaîne :

- sources externes de données de la solution ENT : Annuaire académique fédérateur (AAF), Système d'authentification et de propagation d'identité de l'agriculture (SAPIA), annuaire de la collectivité, etc. ;
- Gestionnaire d'accès aux ressources ;
- services Tiers (fournisseurs de ressources, services locaux d'écoles ou d'établissements, services en ligne du ministère en charge de l'Éducation nationale, de la collectivité...);
- fournisseurs d'identité externes ;
- autres solutions ENT.

Les tests doivent permettre de s'assurer du bon fonctionnement de la solution ENT au sein de son écosystème. En conséquence, les tests fonctionnels **DOIVENT** inclure des scénarios mettant en évidence le fonctionnement correct de la solution ENT en interaction avec les autres composants de son écosystème.

Ces scénarios doivent être joués même si des mises en productions (d'évolutions, de correctifs, etc.) concernent d'autres composants que la solution ENT elle-même.

4.4. Fourniture et évolutions de l'ENT

Afin de fiabiliser la mise en production, d'être en mesure d'atteindre les niveaux de qualité de service fixés et de garantir la pérennité de l'ENT, un certain nombre de directives sont à respecter en amont de la phase d'exploitation, tant au niveau de la contractualisation, que des livrables et des processus.

4.4.1. Fourniture initiale

La fourniture initiale d'un ensemble de services est réalisée par un éditeur et/ou un intégrateur ENT chargé, après la mise en exploitation, de maintenir ces services. Cette phase peut se réduire à une personnalisation de solutions standards (ou de progiciels) déployées dans d'autres établissements ou sur d'autres projets.

La fourniture initiale inclura un ensemble de documentations et de procédures d'installation, d'intégration, de tests, de mise en production et d'exploitation qui devront être mises à jour tout au long des évolutions ultérieures dans le cadre des différentes opérations de maintenance.

Dans le cadre de cette phase initiale dans le cycle de vie de la solution ENT, et dans le cas de solutions d'intégration, l'éditeur / intégrateur ENT **DOIT** mettre au point une procédure de réversibilité, destinée à permettre un changement de titulaire pour la maintenance de la solution ENT, à en renforcer ainsi le niveau de maintenabilité et à en garantir la pérennité. Cette procédure de réversibilité pourra, par ailleurs, être mise en œuvre partiellement ou intégralement lors de l'affectation de nouvelles personnes dans l'équipe de maintenance et garantir ainsi un transfert de compétences efficace.

Cette procédure de réversibilité sera vérifiée et le cas échéant modifiée régulièrement, suivant une périodicité prédéfinie (exemple : à l'ouverture du service, puis annuellement ou à l'occasion de changement de versions majeures des logiciels).

4.4.2. Maintenance

4.4.2.1. Évolution dans le cadre d'une maintenance

La phase de maintenance démarre dès la mise en exploitation de la solution ENT, mais la notion d'évolution n'est pas spécifique à la phase de maintenance. En effet, certaines évolutions sont effectuées au cours du cycle de réalisation après l'identification de spécifications incomplètes, de spécifications imprécises et non comprises de manière idoine par l'intégrateur, de besoins affinés à la relecture des spécifications ou de l'observation du fonctionnement d'une maquette, d'évolutions externes (composants standards, etc.), de nouveaux besoins ou d'inversion de priorités...

La maintenance matérielle prévoit les remplacements / retraits / ajouts / dépannages d'un équipement ou d'un composant matériel.

La maintenance logicielle prévoit les modifications d'un ou plusieurs composants logiciels (exemple : application d'un correctif, changement de version logicielle, modification du paramétrage).

Les opérations de maintenance matérielle et/ou logicielle peuvent être classées en plusieurs catégories : maintenance corrective, adaptative, évolutive, réglementaire, préventive.

4.4.2.1.1. Maintenance corrective

La maintenance corrective vise à mettre en œuvre une procédure ou un moyen technique afin de palier un dysfonctionnement (incident) constaté sur une partie du système d'information.

4.4.2.1.2. Maintenance adaptative

La maintenance adaptative vise à définir un ensemble d'actions de maintenance en vue d'adapter une partie des services de la solution ENT à une modification de l'environnement à venir, interne à la solution ENT (exemple : évolution imposée par la politique de maintenance de l'éditeur d'une version d'un logiciel du système) ou externe (composant interagissant avec la solution ENT : postes de travail externes, réseaux, autres services applicatifs).

4.4.2.1.3. Maintenance évolutive

La maintenance évolutive a pour objet la mise en place de nouveaux services ou l'évolution de ceux déjà présents, améliorant ainsi les services rendus aux utilisateurs et/ou exploitants.

4.4.2.1.4. Maintenance réglementaire

La maintenance réglementaire a pour objet d'apporter des modifications permettant de rendre compatibles les services applicatifs avec de nouvelles directives réglementaires ou normes en vigueur. Elle s'apparente à la maintenance évolutive. Les délais de mise en œuvre peuvent être très contraignants (basculement à une date précise ou délais de réalisation courts).

4.4.2.1.5. Maintenance préventive

La maintenance préventive vise à définir un ensemble d'actions de maintenance (logicielle ou matérielle) ayant pour but de prévenir un dysfonctionnement probable ou possible ou une dégradation du fonctionnement (performances...).

4.4.2.2. Contractualisation

La maintenance corrective et certaines opérations de maintenance préventive, telles que les mises à jour des patches de sécurité, des signatures anti-virus et des actions préventives de maîtrise des performances, **DOIVENT** faire l'objet de forfaits sur la base des niveaux d'engagement de qualité de service souhaités.

Des unités d'œuvre **DEVRAIENT** être introduites dans le contrat pour la réalisation des autres activités de maintenance, afin de garantir une bonne réactivité du titulaire et la maîtrise des coûts.

En tout état de cause, tout prestataire **DOIT** être lié par un document contractuel. Celui-ci **DOIT** notamment contenir les obligations de sécurité et de confidentialité du sous-traitant conformément au RGPD et à la loi relative à l'Informatique, aux fichiers et aux libertés modifiée.

4.4.2.3. Gestion des changements

Une évolution, quelle que soit le domaine de maintenance concerné (corrective, évolutive...), se traduit généralement par un ou plusieurs changements de la plateforme d'exploitation.

Les changements effectués lors des différentes opérations de maintenance (ajout, retrait ou remplacement d'un composant, modification de modules logiciels ou de paramètres...) peuvent avoir, s'ils ne sont pas maîtrisés, un impact négatif sur la qualité de service (coupures de service, instabilité de fonctionnement...), sur la maîtrise de la solution ENT (dégradation du facteur de maintenabilité, perte de connaissance des changements effectués...) ou sur les coûts de projets (mauvaise optimisation des évolutions, surcoûts de non-qualité ou de difficulté d'analyse des incidents par manque de maîtrise des changements, non cohérence...).

Les changements sont, la plupart du temps, planifiables (« changement planifié ») ; ils ne le sont pas dans le cas d'opérations urgentes (« changement urgent ») telles que la résolution d'incidents graves (maintenance corrective) ou la prévention d'incidents graves lors de l'identification de risques importants (seuils d'alarme, nouvelles vulnérabilités...).

Les « demandes standards », c'est-à-dire les opérations prédéfinies, compatibles avec l'environnement de production et dont les coûts et modalités sont également prédéfinies, ne sont pas contrôlées par le processus de gestion des changements. Il s'agit d'opérations « courantes », décrites comme étant permises dans les consignes d'exploitation et, si cela est nécessaire, ayant fait l'objet de tests préalables. Il s'agit, par exemple, d'opérations d'extraction de données, d'opérations d'optimisation des ressources, de changements de l'ordonnancement des traitements par lot (batch), de changements autorisés de paramètres ou de sécurisation de flux...

Il est important de trouver un compromis entre les délais de mise en œuvre et la fréquence des changements, excepté dans le cas des changements urgents.

Des processus permettant la fiabilisation de la mise en production, la maintenabilité et la minimisation des coupures de service **DOIVENT** être définis et appliqués. Toute mise en production, même d'une évolution mineure, **DOIT** faire l'objet de tests préalables, excepté dans de très rares cas où l'urgence prime (alerte importante de sécurité...). Toutes les documentations et procédures impactées par les changements devront être mises à jour, ainsi que les informations de la base de gestion de configurations. Si des changements planifiables impactent la disponibilité de l'ENT lors de périodes d'utilisation ou les modes opératoires des utilisateurs, ces derniers **DOIVENT** être prévenus au préalable (exemple : informations sur le portail ou la messagerie électronique).

Certains changements peuvent nécessiter la mise au point de procédures spécifiques ou l'adaptation de procédures existantes permettant de limiter la durée de rupture de service. Dans certains cas de figure, il est préférable de réaliser le changement en plusieurs étapes ou, dans d'autres, au contraire, de grouper ces étapes (exemple : changements matériels et logiciels). La stratégie de mise en place de ces changements se doit d'être définie et déclinée tout au long du cycle d'exploitation.

L'opération de changement ne doit être close qu'après une courte phase d'observation du comportement de la plateforme suite à l'application de ce changement. En cas d'insuccès, un plan d'actions correctives sera obligatoirement mis en place. Un retour arrière temporaire ou définitif peut être décidé, s'il est techniquement possible de le réaliser (compatibilité de bases...).

Les changements importants peuvent nécessiter une organisation en mode projet et l'intervention d'acteurs multiples (mainteneurs, exploitants, experts...).

Il convient de catégoriser les changements sous deux angles :

- l'urgence du changement, c'est-à-dire l'urgence d'application d'une correction ou de déploiement d'une évolution fonctionnelle ;
- le niveau de complexité du changement, nécessitant une organisation et des processus plus ou moins lourds.

La gestion des changements se fait sous le contrôle d'une personne désignée, faisant partie de l'équipe de maîtrise globale de la solution ENT, dont les objectifs sont :

- de s'assurer que les changements sont contrôlés et respectent les procédures normalisées ;
- d'éviter les changements non contrôlés ou non justifiés ;
- d'assurer une cohérence au niveau des évolutions, les sources des changements pouvant être variées ;
- de gérer les priorités des changements et améliorer ainsi la réactivité pour ceux jugés urgents ;
- de gérer les risques et d'en améliorer leur analyse ;
- de limiter les interruptions de service et de fiabiliser les mises en productions ;
- de faciliter la maintenabilité et la gestion des incidents ;
- d'optimiser les coûts et améliorer la productivité.

Dans le cas du choix d'un prestataire extérieur unique pour l'hébergement et la maintenance, le contrat peut préciser un niveau de délégation à ce prestataire pour la gestion des changements liés à des opérations de maintenance corrective ou préventive.

4.4.3. Les étapes préalables à une mise en exploitation

La mise en production d'une solution ENT ou d'une évolution majeure **DOIT** être précédée par une phase de tests et de recette (Vérification d'aptitude au bon fonctionnement – VABF) chargée de valider la solution à déployer, les procédures et outils de mise en exploitation et d'exploitation. Après la recette formelle (VABF), la période de Vérification de service régulier (VSR) permet de vérifier le bon fonctionnement de la solution ENT et son exploitabilité en conditions réelles.

Après la mise en exploitation de la solution ENT, et le passage du projet en mode de maintenance, tout changement doit alors suivre ce même cycle ou un cycle simplifié en fonction de la complexité et du niveau de risque de ce changement.

Un PAQ (Plan d'Assurance Qualité) sera exigé de chaque fournisseur retenu pour les différentes prestations : fourniture de la solution ENT, maintenance et hébergement. Il indique les dispositions mises en œuvre pour garantir la satisfaction des exigences du projet, notamment en termes de moyens, procédures, méthodes, ainsi que par l'indication des rôles et responsabilités de chacun.

4.4.4. Livrables

Les livrables fournis lors des phases du cycle de vie de projet d'intégration **DOIVENT** au minimum se composer de :

- documentations d'architecture et de spécifications techniques et fonctionnelles ;
- documentation du dimensionnement de la plateforme, dossiers d'exploitation et toute autre documentation nécessaire à la maintenance de la solution ENT (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ;
- procédures de mise en exploitation et documentations associées : procédure d'installation / réinstallation et/ou de migration, procédures de retour arrière, procédures de vérification du bon fonctionnement après installation ou migration (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ;
- procédures d'exploitation et documentations associées, notamment surveillance, procédures d'installation et de relance unitaire des services, procédures de reconstitution ou remise en ordre de tout ou partie de la plateforme, procédures de sauvegardes et de restauration, analyses de traces, aide au diagnostic (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ;
- documentations de tests et résultats des tests effectués ;
- notes de version pour les maintenances correctives et évolutives (qui peuvent être communiquées aux utilisateurs après la mise en œuvre de la version).

Ces documentations sont destinées notamment aux mainteneurs et aux exploitants de la solution ENT. La complétude et l'exactitude de ces documentations devra être une des conditions de recette du fournisseur (VABF).

Le mainteneur et l'exploitant **DOIVENT** garantir la mise à jour de l'ensemble de ces livrables lors de toute action d'évolution. Le processus d'évolution des documents **DOIT** être inscrit dans celui de la gestion des changements.

Les procédures de réinstallation de tout ou partie de plateforme ne se limitent pas à des procédures unitaires d'installation de chacun des composants. Après une opération lourde de maintenance matérielle ou logicielle ou après certains incidents, la remise en fonctionnement de la plateforme devra, dans la majorité des cas, s'effectuer selon un processus qui aura été préalablement validé, afin de garantir une remise en cohérence de la plateforme en composants et en données tout en limitant le temps d'interruption de service.

Ce processus de remise en fonctionnement consiste en un ensemble de consignes précises et bien décrites à exécuter dans un ordre et un cadencement établis selon des conditions dûment énoncées.

De la sorte l'exploitant et tous ses intervenants seront à même d'intervenir le plus rapidement possible, notamment dans les opérations non programmées de résolution d'incidents, en appliquant strictement la procédure recommandée, sans avoir à chercher des informations ou faire appel aux mainteneurs et sans risquer de mauvaises manipulations. Les délais de remise en fonctionnement de la plateforme, incluant le cas échéant les délais de restauration des données, auront préalablement été estimés et communiqués.

Les consignes d'exploitation **DOIVENT** être enrichies au cours de la phase d'exploitation à partir des retours d'expérience dans les domaines de la résolution d'incidents et de la remise en service : optimisation, simplification, etc. L'objectif de ce processus est de diminuer les temps de résolution et les temps d'indisponibilité pour améliorer continuellement la qualité de service des versions stabilisées.

4.4.5. Tests

Toute mise en production d'une version majeure ou mineure ou tout changement **DOIT** faire l'objet de tests préalables sur au moins une plateforme, selon un processus adapté à chacune des typologies d'évolution.

Les tests sont conduits par l'intégrateur ou le mainteneur de la solution, à l'exception de ceux relatifs aux évolutions maîtrisées par l'exploitant (exemple : application de correctifs de sécurité ou de logiciels de base des systèmes, en relation avec les éditeurs ou constructeurs des composants matériels). Dans ce dernier cas, l'exploitant se doit d'informer le mainteneur du résultat des tests et de l'évolution réalisée.

Les tests et la stratégie de tests **DOIVENT** être documentés et transmis à la maîtrise d'ouvrage du projet ENT.

Lors de changements mineurs concernant notamment les opérations légères de maintenance corrective ou préventive ne faisant pas l'objet d'une recette formelle et dont les risques estimés sont faibles, les tests effectués ont pour objet de tester l'évolution. Le cas échéant, si l'évolution peut avoir des impacts sur d'autres fonctions de l'ENT, ces tests **DOIVENT** être complétés par quelques scénarios de tests de non-régression représentatifs préétablis.

Lors de changements moyens ou majeurs, un plan de tests **DOIT** être établi par le mainteneur. Ce plan de tests comprend des tests spécifiques de validation des évolutions et d'une liste soigneusement présélectionnée de tests de non-régression suivant les impacts des évolutions sur les modules existants.

Seules les évolutions réalisées dans le cadre de la maintenance corrective et une partie des opérations de maintenance préventive **PEUVENT** ne pas faire l'objet de recette formelle (VABF et VSR).

Les tests à effectuer ne se limitent pas à la vérification fonctionnelle des services de l'ENT. Toutes les procédures de mise en exploitation **DOIVENT** être testées et, notamment :

- les procédures d'installation et de migration ;
- les procédures de reprise en cas d'incidents graves (basculement des traitements sur une des unités centrales du système redondé) ;
- les procédures et enchaînements de procédures (consignes) de remise en ordre de marche manuelle de tout ou partie de la plateforme de production ;
- les procédures de sauvegardes et de restaurations ;
- les procédures de supervision ;
- les procédures de mise en exploitation et, le cas échéant, de migration, les tests de vérification de la mise en exploitation, ainsi que les éventuelles procédures de retour arrière en cas d'insuccès.

Les tests de non-régression et la stratégie de test **DOIVENT**, si nécessaire, évoluer en fonction des incidents rencontrés en exploitation et des retours d'expérience.

Des tests de performance **DOIVENT** permettre de calibrer la plateforme avant une mise en exploitation, d'optimiser les paramétrages et d'affiner le dossier de dimensionnement de la plateforme. Des scénarios représentatifs des grandes fonctionnalités seront définis avec la maîtrise d'ouvrage et testés unitairement et en charge pendant la campagne de tests. Ces mêmes scénarios seront utilisés pour l'évaluation de la qualité de service en exploitation. Chaque soumissionnaire à la fourniture d'une solution ENT devra préciser dans sa réponse les moyens qu'il prévoit de mettre en œuvre pour la réalisation des tests de performances et le dimensionnement de la plateforme.

La durée de batch éventuels **DOIT** être estimée afin d'optimiser la planification de leur exécution, pendant les périodes de faible charge.

4.4.6. Définition du planning de déploiement

La première mise en exploitation d'une solution ENT **DEVRAIT** se faire progressivement (exemple : déploiement pilote, déploiement généralisé dans un nombre limité d'établissements, généralisation progressive ou groupée dans les autres établissements).

Un déploiement **NE DEVRAIT PAS** être planifié lors des périodes critiques ou de forte affluence (exemple : rentrée scolaire). Les contraintes calendaires de l'ENT étant nombreuses (marchés publics, fonctionnement des collectivités, délais des prestataires et fournisseurs, niveau de risque de non-respect du planning...), une attention particulière sera portée aux aspects contractuels relatifs à la définition des objectifs calendaires et des engagements de planning demandés aux prestataires extérieurs.

4.4.7. Gestion de projet et des risques en phase de maintenance et d'exploitation

La gestion de projet ne doit pas s'arrêter à la mise en exploitation d'une solution ENT. Elle doit se poursuivre lors du cycle de maintenance de la solution ENT. La fréquence et l'organisation des comités s'adapteront à cette phase. La gestion des changements majeurs peut s'inscrire dans l'ordre du jour de ces mêmes comités. Ces comités peuvent également traiter les évolutions qui nécessitent l'élaboration de cahiers des charges et de devis des prestataires (exemple : maintenance évolutive).

4.4.8. Audits

Chacun des acteurs de réalisation, de maintenance ou d'exploitation d'une solution ENT est susceptible d'être audité. Les audits peuvent être des audits de sécurité, de qualité des réalisations technologiques (exemple : audit du code, audit des procédures d'exploitation ou de mesure des indicateurs...) ou de contrôle de la qualité des processus mis en œuvre (vérification des processus documentés et/ou de leur application).

4.4.9. Réversibilité

Pour différentes raisons, la maintenance et/ou l'exploitation de la solution ENT doivent pouvoir être transférées à un nouveau prestataire (en fin de marché ou de manière anticipée dans le cas d'une résiliation). Les modalités de réversibilité **DOIVENT** être définies dans les contrats.

La réversibilité peut aussi être mise en œuvre lors d'un changement de solution applicative sans changement de prestataire pour des raisons de maintenance et d'exploitation.

Une phase de réversibilité sera déclenchée suivant un plan de réversibilité mis au point par le titulaire d'origine. Les deux marchés cohabiteront alors pendant une courte phase de transition dont l'objet est le transfert de compétences, la transmission des contenus, la communication des tickets de support en cours et la bascule des responsabilités.

Le porteur de projet **DEVRAIT** demander au nouveau titulaire d'établir, avant la fin de cette phase, une analyse de risques argumentée.

Pour rappel, les plans de réversibilité, de maintenance et d'exploitation doivent être mis à jour de manière régulière et, notamment, à l'occasion de changements importants.

Le plan de réversibilité **DOIT** décrire :

- l'organisation à mettre en place ;
- la répartition des responsabilités ;
- la structuration de cette phase (étapes, relations entre les étapes et conditions de fin d'étape) ;
- les éléments de délais et de contraintes de planning ;
- la description de l'assistance administrative et technique et du transfert de compétences ;
- la liste des éléments à transférer et les modalités de transfert ;
- l'ensemble des traitements appliqués aux données provenant de comptes supprimés ou en instance de suppression ;
- les données de l'ENT éligibles à la reprise dans le cas où le plan de réversibilité comporterait des changements à risque pour l'intégrité de ces données (par exemple un changement de solution ENT ou un changement d'hébergement).

Le volume et la variété des données éligibles à la reprise en cas de réversibilité est un paramètre d'ajustement sur le coût de la réversibilité. Pour chaque type de donnée, la maîtrise d'ouvrage en charge du projet ENT pourra juger de son intérêt de leur reprise, en particulier si la réversibilité se déroule en fin d'année scolaire (ce qui est souvent le cas).

Le plan de réversibilité **DEVRAIT** être vérifié de manière périodique ou lors de changements importants.

La mise en œuvre du plan de réversibilité dans un projet ENT **NE DEVRAIT PAS** avoir d'impact sur les données de l'ENT. Dans le cas où le plan de réversibilité induit un changement présentant un risque sur l'intégrité des données de l'ENT (changement de solution ENT, changement d'hébergement, changement de l'exploitant, changement de l'hébergeur...), le nouveau prestataire (intégrateur/éditeur/mainteneur) **DOIT** garantir l'intégrité des données de l'ENT. Pour cela, il **PEUT** exploiter les capacités d'import / export des solutions ENT.

Si l'ancien intégrateur/éditeur/mainteneur n'a pas d'engagement de mise à disposition des données de l'ENT pour leur reprise, le nouvel intégrateur/éditeur/mainteneur **DOIT** estimer les charges associées à la migration des données éligibles à la reprise.

Lors de la mise en place d'un marché ENT, le nouvel intégrateur/éditeur/mainteneur **DOIT** s'engager, en cas de réversibilité future, à mettre à disposition du projet toutes les données éligibles à la reprise dans un délai raisonnable (à estimer selon la volumétrie) et ce, dans un **format standard** ou reconnu et éprouvé s'il existe et est adapté ou, à défaut, dans un **format ouvert, structuré, documenté et outillé**. Cette mise à disposition **DOIT** être faite dans un délai raisonnable (à estimer en fonction de la volumétrie des données). Le nouvel intégrateur/éditeur/mainteneur **DOIT** également décrire dans le plan de réversibilité les mécanismes et les outils qui seront utilisés pour la mise à disposition des données éligibles à la reprise et estimer les coûts associés.

4.4.10. Changement de solution ENT

Les changements de solution ENT jalonnent la vie des projets ENT. Ils peuvent intervenir pour différents motifs (changement de marché, nécessité d'une mise à niveau majeure de la solution, application de la clause de réversibilité, changement d'hébergement...).

Du point de vue de l'intégrité des données de l'ENT, ces changements devraient être autant que possible transparents et permettre aux utilisateurs de retrouver la plupart de leurs anciennes données dans la nouvelle solution. Par exemple, les élèves devraient pouvoir y retrouver leurs productions, les enseignants leurs mails, leurs données de cahier de textes ainsi que leurs parcours pédagogiques, les chefs d'établissement leurs mails et leur agenda, etc. Les données de l'ENT (documents, réservations...) autres que celles des utilisateurs doivent aussi se retrouver dans la nouvelle solution.

Cependant, sur le terrain, il arrive parfois que de tels changements conduisent à ce que des données ne puissent être récupérées, ce qui engendre une dépréciation et peut avoir un impact négatif sur la perception des utilisateurs (expérience utilisateur perçue). Si les exigences et les modalités de reprise des données de l'ENT sont négligées ou insuffisamment prises en compte lors de la rédaction du marché, il existe un fort risque de démotivation pour les utilisateurs de l'ENT et par conséquent, d'un impact potentiel négatif sur les usages.

Afin d'éviter ce risque, le cahier des charges devrait préciser la liste des données éligibles à la reprise ainsi que leurs conditions de récupération (services concernés, volumétrie à prendre en compte, priorité, délai de mise à disposition...).

D'un point de vue opérationnel, la reprise des données éligibles ne sera possible que si l'ancienne solution est capable de mettre les données à disposition de la nouvelle solution (export / import de données).

Lors d'un changement de solution d'un projet ENT, la nouvelle solution **DEVRAIT** permettre aux utilisateurs de retrouver leurs données (éligibles à la reprise) dans l'ENT dans les mêmes conditions d'exploitabilité que dans l'ancienne solution :

- s'il s'agit d'un changement de marché ENT, le nouvel intégrateur/éditeur/mainteneur **DEVRAIT** prendre l'engagement de la reprise dans la nouvelle solution des données existantes et ce, dans un délai raisonnable (à estimer par l'intégrateur/éditeur/mainteneur en fonction de la taille du projet et de la volumétrie des données concernées). Si l'ancien intégrateur/éditeur/mainteneur n'est pas tenu par un engagement pour mettre à disposition du projet les données éligibles à la reprise, il sera nécessaire de prévoir cette activité comme un prérequis dans le nouveau marché ;
- s'il s'agit d'un renouvellement de marché ENT ou d'un changement de solution au sein du même marché, l'intégrateur/éditeur/mainteneur actuel **DEVRAIT** prendre l'engagement de la migration des données éligibles à la reprise depuis l'ancienne solution vers la nouvelle solution.

Dans les deux cas cités, afin d'anticiper de futurs changements de solution ENT, l'intégrateur/éditeur/mainteneur de la nouvelle solution **DEVRAIT** être en mesure, pendant la durée du marché, de mettre à disposition du projet toutes les données éligibles à la reprise, et ce dans un format standard ou reconnu et éprouvé s'il existe et adapté ou, à défaut, dans un format ouvert, structuré, documenté et outillé. Cette mise à disposition **DEVRAIT** être réalisée dans un délai raisonnable (à estimer selon la volumétrie des données).

De la même manière, l'intégrateur/éditeur/mainteneur de la nouvelle solution ENT **DEVRAIT** s'engager à fournir la documentation complète des formats d'import et d'export utilisés et supportés par la solution ENT mise en œuvre dans le projet.

En cas de développement spécifique nécessaire pour assurer la reprise dans la nouvelle solution de certaines données éligibles, l'intégrateur/éditeur/mainteneur de la nouvelle solution **DEVRAIT** s'appuyer sur la documentation fournie par les éditeurs ENT. L'intégrateur/éditeur/mainteneur **DEVRAIT** s'appuyer pour ces développements sur les capacités d'import / export de données de la solution ou développer des fonctionnalités spécifiques.

En cas de développement spécifique nécessaire pour assurer la migration de certaines données éligibles à la reprise, l'intégrateur/éditeur/mainteneur en charge de la nouvelle solution **DEVRAIT** fournir dans sa proposition une estimation de la charge de travail et des coûts pour ce développement en cas de réversibilité, de changement de solution ou de changement d'année scolaire (si elle n'est pas prise en compte nativement par la solution ENT proposée).

Les projets ENT devront prendre en compte dans leur budget et dans leur analyse des propositions les différentes estimations fournies par l'intégrateur/éditeur/mainteneur et les conditions financières associées.

Le Tableau 8 donne un exemple de priorisation des données éligibles à la reprise (d'après des informations recueillies auprès d'un échantillon d'acteurs du terrain).

Priorité	Service de l'ENT (cf. architecture de référence présentée dans le document principal du SDET)	Donnée éligible à la reprise
1	Cahier de textes / cahier journal [UTI-AVE-CDT]	Cahier de textes personnel de l'enseignant (2D)
1	Cahier de textes / cahier journal [UTI-AVE-CDT]	Cahier journal de l'enseignant (1D)
2	Espaces d'échanges et de collaboration [UTI-CCO-EEC]	Données d'espaces d'échange et de collaboration
2	Espace de stockage et de partage de fichiers [UTI-UTL-ESF]	Données personnelles de l'espace personnel de stockage et de partage (fichiers)
2	Publication Web [UTI-CCO-PWE]	Données de publication Web
2	Courrier électronique [UTI-CCO-CEL]	Courrier électronique
3	Construction et gestion de parcours pédagogiques [UTI-PPE-CGP]	Parcours pédagogiques (format IMS CC)
4	Construction et gestion de parcours pédagogiques [UTI-PPE-CGP]	Parcours pédagogiques (format SCORM)
5	Gestion des signets [UTHDO-GSI]	Données de signets
5	Gestion de groupes d'utilisateurs [UTI-UTL-GRP]	Données de gestion des groupes d'utilisateurs
6	Conférence audio et vidéo [UTI-CCO-CAV]	Données enregistrées de conférences audio et vidéo
6	Pages blanches [UTHDO-PBL]	Pages blanches
6	Réservation de salles et matériels [UTI-UTL-RES]	Réservation de salles et de matériels (historique et réservations en cours)
6	Réservation de salles et matériels [UTI-UTL-RES]	Ressources matérielles de l'établissement déclarées dans l'ENT
7	Agendas [UTHDO-AGE]	Agenda du chef d'établissement

Tableau 8 : Exemple de priorisation pour la reprise et la portabilité de données de l'ENT

En complément des données définies par le projet comme éligibles à la reprise en cas de changement de solution ou d'application de la réversibilité, certaines données techniques sont indispensables pour assurer le bon fonctionnement de l'ENT ; c'est le cas de l'identifiant unique dédié à l'interfaçage avec le GAR, le `GARPersonIdentifiant`.

En effet, le `GARPersonIdentifiant` permet au GAR de faire le rapprochement entre les utilisateurs de l'ENT et les ressources qui leur sont affectées.

En cas de changement de solution ENT, le `GARPersonIdentifiant` **DOIT** être conservé pour tous les comptes utilisateurs pour lesquels il est défini.

En cas de changement de solution ENT, l'intégrateur/éditeur/mainteneur de la nouvelle solution ENT **DOIT** s'assurer que le GARPersonIdentifiant de chaque compte utilisateur est bien récupéré et associé au compte dans la nouvelle solution lors de la reprise de données depuis l'ancienne solution.

En cas d'application du plan de réversibilité, le nouveau prestataire (intégrateur/éditeur/mainteneur) **DOIT** garantir le maintien de l'association des GARPersonIdentifiant et des comptes utilisateurs dans l'ENT.

De la même manière, un utilisateur **DOIT** conserver le même GARPersonIdentifiant tant qu'il reste sur le même projet ENT.

En cas de suppression d'un compte dans l'ENT, le GARPersonIdentifiant **NE DOIT** jamais être réattribué à un autre utilisateur sauf s'il s'agit du même utilisateur qui revient dans l'ENT et que le projet ENT autorise sa réattribution.

4.5. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Contractualisation	Les objectifs de qualité de service DOIVENT être déclinés sous forme d'engagements personnalisés fixés à chacun des acteurs et contractants en fonction de leur domaine de responsabilité.	E	E
02	Contractualisation	La maîtrise d'ouvrage du projet ENT DEVRAIT limiter le nombre de contrats passés avec des prestataires extérieurs, à charge pour ces derniers de sous-traiter des tâches spécifiques à d'éventuels partenaires.	R	R
03	Contractualisation	Une clause de réversibilité et une obligation de mise à disposition des documentations actualisées DOIVENT être prévues au contrat avec l'intégrateur/éditeur initial.	E	E
04	Contractualisation	La maintenance PEUT être confiée à un acteur différent de l'intégrateur/éditeur initial lorsque la mise en œuvre de la solution ENT est stabilisée.	F	F
05	Responsabilités	Toutes les activités d'exploitation PEUVENT être confiées à l'hébergeur/exploitant, y compris toutes celles relatives à l'exploitation des services applicatifs (ex : maintenance des bases de données...).	F	F
06	Responsabilités	L'intégrateur/éditeur/mainteneur DOIT produire une étude de dimensionnement qui indique les conditions dans lesquelles il garantit la qualité de service demandée compte tenu de la volumétrie et des exigences du projet ENT.	E	E
07	Prévention des risques	Des campagnes de tests de performance DEVRAIENT être menées avant la mise en production de nouvelles versions applicatives.	R	R
08	Contractualisation	L'exploitation et la maintenance de la solution ENT PEUVENT être confiées au même prestataire.	F	F

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
09	Propriété des matériels et logiciels	Si du matériel ou des logiciels faisant partie de la solution ENT sont la propriété du porteur de projet, ce dernier DOIT donner aux exploitants et mainteneurs l'accès au support prévu dans les contrats de maintenance signés pour ces logiciels ou matériels.	E	E
10	Propriété des matériels et logiciels	Si les composants matériels et logiciels sont la propriété d'un prestataire engagé sur un niveau de qualité de service dans un contexte technique et fonctionnel et sur une volumétrie d'utilisation définis dans le contrat, le prestataire DOIT alerter suffisamment à l'avance la maîtrise d'ouvrage du projet ENT de la nécessité de faire évoluer les composants logiciels et matériels pour maintenir une qualité de service élevée et DOIT indiquer ses recommandations d'évolutions de la solution ENT.	E	E
11	Propriété des matériels et logiciels	Si les composants matériels et logiciels sont la propriété d'un prestataire responsable de l'évolution des composants logiciels et matériels, le mode de financement de ce prestataire DOIT dans ce cas être adapté en conséquence.	E	E
12	Propriété des matériels et logiciels	Si les droits patrimoniaux des développements spécifiques des services applicatifs ne sont pas transférés à la maîtrise d'ouvrage du projet ENT (cas notamment des offres SaaS), le contrat DOIT contenir une clause permettant d'assurer la pérennité de l'ENT en cas de défaillance du prestataire ou arrêt de maintenance des logiciels (dépôt des sources, accès aux sources...).	E	E
13	Réversibilité	Tout contrat avec un prestataire extérieur DOIT pouvoir être résilié pour manquement de l'une ou l'autre des parties ou pour non-respect chronique des niveaux de service contractualisés.	E	E
14	Réversibilité	Le contrat DOIT exiger une garantie de bonne fin, en fin de marché ou après résiliation, incluant une clause de réversibilité.	E	E
15	Contractualisation	Le contrat DOIT établir clairement les domaines de responsabilité, les objectifs de qualité de service et les indicateurs de mesure associés.	E	E
16	Plateformes	Un cloisonnement de la plateforme de production DOIT être mis en place afin d'empêcher le moindre accès aux données de la solution ENT à partir d'une des autres plateformes.	E	E
17	Plateformes	Les tests fonctionnels DOIVENT inclure des scénarios mettant en évidence le fonctionnement correct de la solution ENT en interaction avec les composants de son écosystème : sources externes de données de la solution ENT (AAF, SAPIA, annuaire de la collectivité, etc.), Gestionnaire d'accès aux ressources, services Tiers (fournisseurs de ressources, services locaux d'écoles ou d'établissements, services en ligne du ministère en charge de l'Éducation nationale, de la collectivité, etc.), fournisseurs d'identité externes, autres solutions ENT...	E	E
18	Réversibilité	L'intégrateur/l'éditeur DOIT mettre au point une procédure de réversibilité destinée à permettre un changement de titulaire pour la maintenance de la solution ENT, à en renforcer ainsi le niveau de maintenabilité et à en garantir la pérennité.	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
19	Contractualisation	La maintenance corrective et certaines opérations de maintenance préventive, telles que les mises à jour des patchs de sécurité, des signatures anti-virus et des actions préventives de maîtrise des performances, DOIVENT faire l'objet de forfaits sur la base des niveaux d'engagement de qualité de service souhaités.	E	E
20	Contractualisation	Des unités d'œuvre DEVRAIENT être introduites dans le contrat pour la réalisation des autres activités de maintenance, afin de garantir une bonne réactivité du titulaire et la maîtrise des coûts. En tout état de cause, tout prestataire DOIT être lié par un document contractuel. Celui-ci DOIT notamment contenir les obligations de sécurité et de confidentialité du sous-traitant conformément au RGPD et à la loi n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés modifiée.	R	R
21	Maintenance	Des processus permettant la fiabilisation de la mise en production, la maintenabilité et la minimisation des coupures de service DOIVENT être définis et appliqués.	E	E
22	Maintenance	Toute mise en production, même d'une évolution mineure, DOIT faire l'objet de tests préalables, excepté dans de très rares cas où l'urgence prime (alerte importante de sécurité...).	E	E
23	Maintenance	Si des changements planifiables impactent la disponibilité de l'ENT lors de périodes d'utilisation ou les modes opératoires des utilisateurs, ces derniers DOIVENT être prévenus au préalable.	E	E
24	Mise en exploitation	La mise en production d'une solution ENT ou d'une évolution majeure ou d'un changement survenu après la mise en exploitation DOIT être précédée par une phase de tests et de recette chargée de valider la solution à déployer, les procédures et outils de mise en exploitation et d'exploitation.	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
25	Livrables	<p>Les livrables fournis lors des phases du cycle de vie de projet d'intégration DOIVENT au minimum se composer de :</p> <ul style="list-style-type: none"> ▪ documentations d'architecture et de spécifications techniques et fonctionnelles ; ▪ documentation du dimensionnement de la plateforme, dossiers d'exploitation et toute autre documentation nécessaire à la maintenance de la solution ENT (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ; ▪ procédures de mise en exploitation et documentations associées : procédure d'installation et/ou de migration, procédures de retour arrière, procédures de vérification du bon fonctionnement après installation ou migration (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ; ▪ procédures d'exploitation et documentations associées, notamment surveillance, procédures d'installation et de relance unitaire des services, procédures de reconstitution ou remise en ordre de tout ou partie de la plateforme, procédures de sauvegardes et de restauration, analyses de traces, aide au diagnostic (la fourniture de ces livrables à la maîtrise d'ouvrage n'est pas obligatoire dans le cas d'une solution proposée en mode SaaS) ; ▪ documentations de tests et résultats des tests effectués ; ▪ notes de version pour les maintenances correctives et évolutives (qui peuvent être communiquées aux utilisateurs après la mise en œuvre de la version). 	E	E
26	Livrables	Le mainteneur et l'exploitant DOIVENT garantir la mise à jour de l'ensemble de ces livrables lors de toute action d'évolution.	E	E
27	Gestion de projet	Le processus d'évolution des documents DOIT être inscrit dans celui de la gestion des changements.	E	E
28	Livrables	Les consignes d'exploitation DOIVENT être enrichies au cours de la phase d'exploitation à partir des retours d'expérience dans les domaines de la résolution d'incidents et de la remise en service : optimisation, simplification, etc.	E	E
29	Tests	Toute mise en production d'une version majeure ou tout changement DOIT faire l'objet de tests préalables sur au moins une plateforme, selon un processus adapté à chacune des typologies d'évolution.	E	E
30	Livrables	Les tests et la stratégie de tests DOIVENT être documentés y compris les scénarios de tests de non régression.	E	E
31	Tests	Lors de changements moyens ou majeurs, un plan de tests DOIT être établi par le mainteneur.	E	E
32	Tests	Seules les évolutions réalisées dans le cadre de la maintenance corrective et une partie des opérations de maintenance préventive PEUVENT ne pas faire l'objet de recette formelle (VABF et VSR).	F	F
33	Tests	Toutes les procédures de mise en exploitation DOIVENT être testées.	E	E
34	Tests	Les tests de non-régression et la stratégie de test DOIVENT , si nécessaire, évoluer en fonction des incidents rencontrés en exploitation et des retours d'expérience.	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
35	Tests	Des tests de performance DOIVENT permettre de calibrer la plateforme avant une mise en exploitation, d'optimiser les paramétrages et d'affiner le dossier de dimensionnement de la plateforme.	E	E
36	Tests	La durée de batch éventuels DOIT être estimée afin d'optimiser la planification de leur exécution, pendant les périodes de faible charge.	E	E
37	Déploiement	La mise en exploitation initiale d'une solution ENT DEVRAIT se faire progressivement (exemple : déploiement pilote, déploiement généralisé dans un nombre limité d'établissements, généralisation progressive ou groupée dans les autres établissements).	R	R
38	Déploiement	Un déploiement NE DEVRAIT PAS être planifié lors des périodes critiques ou de forte affluence.	R	R
39	Réversibilité	Pour différentes raisons, la maintenance et/ou l'exploitation de la solution ENT doivent pouvoir être transférées à un nouveau partenaire (en fin de marché ou de manière anticipée dans le cas d'une résiliation). Les modalités de réversibilité DOIVENT être définies dans les contrats.	E	E
40	Réversibilité	La maîtrise d'ouvrage du projet ENT DEVRAIT demander au nouveau titulaire d'établir, avant la fin de la phase de réversibilité, une analyse de risques argumentée.	R	R

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
41	Réversibilité	Le plan de réversibilité DOIT décrire : <ul style="list-style-type: none"> ▪ l'organisation à mettre en place ; ▪ la répartition des responsabilités ; ▪ la structuration de cette phase (étapes, relations entre les étapes et conditions de fin d'étape) ; ▪ les éléments de délais et de contraintes de planning ; ▪ la description de l'assistance administrative et technique et du transfert de compétences ; ▪ la liste des éléments à transférer et les modalités de transfert ; ▪ l'ensemble des traitements appliqués aux données provenant de comptes supprimés ou en instance de suppression ; ▪ les données de l'ENT éligibles à la reprise dans le cas où le plan de réversibilité comporterait des changements à risque pour l'intégrité de ces données (par exemple un changement de solution ENT ou un changement d'hébergement). 	E	E
42	Réversibilité	Le plan de réversibilité DEVRAIT être vérifié de manière périodique ou lors de changements importants. La réversibilité peut aussi être mise en œuvre lors d'un changement de solution applicative sans changement de prestataire pour des raisons de maintenance et d'exploitation.	R	R
43	Réversibilité	La mise en œuvre du plan de réversibilité dans un projet ENT NE DEVRAIT PAS avoir d'impact sur les données de l'ENT.	R	R
44	Réversibilité	Dans le cas où le plan de réversibilité induit un changement présentant un risque sur l'intégrité des données de l'ENT (changement de solution ENT, changement d'hébergement, changement de l'exploitant, changement de l'hébergeur...), le nouveau mainteneur DOIT garantir l'intégrité des données de l'ENT. Pour cela, il PEUT exploiter les capacités d'import / export des solutions ENT.	E	E
45	Réversibilité	En cas d'application de la clause de réversibilité, s'il existe un risque pour les données de l'ENT et que l'ancien mainteneur n'a pas d'engagement pour la mise à disposition des données de l'ENT pour leur reprise, le nouveau mainteneur DEVRAIT estimer les charges associées à la migration des données éligibles à la reprise.	R	R
46	Changement de solution ENT	En cas de changement de la solution d'un projet ENT, la nouvelle solution DEVRAIT permettre aux utilisateurs de retrouver leurs données (éligibles à la reprise) dans l'ENT dans les mêmes conditions d'exploitabilité que dans l'ancienne solution.	R	R
47	Changement de solution ENT	S'agissant d'un changement de marché ENT, le nouvel intégrateur/éditeur/mainteneur DEVRAIT prendre l'engagement de la reprise dans la nouvelle solution des données existantes et ce, dans un délai raisonnable (à estimer par le nouvel intégrateur/éditeur/mainteneur en fonction de la taille du projet et de la volumétrie des données concernées). Si l'ancien intégrateur/éditeur/mainteneur n'a pas d'engagement pour mettre à disposition du projet les données éligibles à la reprise, il sera nécessaire de prévoir cette activité comme prérequis dans le nouveau marché.	R	R

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
48	Changement de solution ENT	S'agissant d'un renouvellement de marché ENT ou d'un changement de solution au sein du même marché, l'intégrateur/éditeur/mainteneur actuel DEVRAIT prendre l'engagement de la migration des données éligibles à la reprise depuis l'ancienne solution vers la nouvelle solution.	R	R
49	Changement de solution ENT	Afin d'anticiper des futurs changements de solution ENT, l'intégrateur/éditeur/mainteneur de la nouvelle solution DEVRAIT être en mesure, pendant la durée du marché, de mettre à disposition du projet toutes les données éligibles à la reprise, et ce dans un format standard ou reconnu et éprouvé s'il existe et est adapté ou, à défaut, dans un format ouvert, structuré, documenté et outillé. Cette mise à disposition DEVRAIT être faite dans un délai raisonnable (à estimer selon la volumétrie des données).	R	R
50	Changement de solution ENT	En cas de changement d'ENT, l'intégrateur/éditeur/mainteneur de la nouvelle solution DEVRAIT s'engager à fournir la documentation complète des formats d'import et d'export utilisés et supportés par la solution ENT mise en œuvre sur le projet.	R	R
51	Changement de solution ENT	En cas de développement spécifique nécessaire pour assurer la reprise dans la nouvelle solution de certaines données éligibles, l'intégrateur/éditeur/mainteneur de la nouvelle solution DEVRAIT s'appuyer sur la documentation fournie par les éditeurs ENT. L'intégrateur/éditeur/mainteneur DEVRAIT s'appuyer pour ces développements sur les capacités d'import / export de données de la solution ou développer des fonctionnalités spécifiques.	R	R
52	Changement de solution ENT	En cas de développement spécifique nécessaire pour assurer la migration de certaines données éligibles à la reprise, l'intégrateur/éditeur/mainteneur en charge de la nouvelle solution DEVRAIT fournir dans sa proposition une estimation financière et de charge de travail pour ce développement en cas de réversibilité, de changement de solution ou de changement d'année scolaire (si elle n'est pas prise en compte nativement par la solution ENT proposée).	R	R
53	GARPersonIdentifiant	En cas de changement de solution ENT, le GARPersonIdentifiant DOIT être conservé pour tous les comptes utilisateurs pour lesquels il est défini.	E	E
54	GARPersonIdentifiant	En cas de changement de solution ENT, l'intégrateur/éditeur/mainteneur de la nouvelle solution ENT DOIT s'assurer que le GARPersonIdentifiant de chaque compte utilisateur est bien récupéré et associé au compte dans la nouvelle solution lors de la reprise de données depuis l'ancienne solution.	E	E
55	GARPersonIdentifiant	En cas d'application du plan de réversibilité, le nouveau prestataire (intégrateur/éditeur/mainteneur) DOIT garantir le maintien de l'association des GARPersonIdentifiant et des comptes utilisateurs dans l'ENT.	E	E
56	GARPersonIdentifiant	Un utilisateur DOIT conserver le même GARPersonIdentifiant tant qu'il reste dans le même projet ENT.	E	E
57	GARPersonIdentifiant	En cas de suppression d'un compte dans l'ENT, le GARPersonIdentifiant NE DOIT jamais être réattribué à un autre utilisateur sauf s'il s'agit d'un utilisateur qui revient dans l'ENT et que le projet ENT autorise sa réattribution.	E	E

Tableau 9 : Exigences et recommandations concernant la stratégie d'exploitation

5. Nomenclatures

5.1. Introduction

L'interopérabilité est un enjeu fort pour les ENT et, comme illustré dans le document principal¹¹, elle se joue sur plusieurs plans :

- niveau politique : partenaires de coopération présentant des projets compatibles, des priorités harmonisées et des objectifs ciblés;
- niveau juridique : harmonisation de la législation pour que les données échangées se voient reconnaître une valeur juridique adéquate;
- niveau organisationnel : processus coordonnés au sein desquels différentes organisations parviennent à un objectif préalablement fixé et offrant un avantage mutuel;
- niveau sémantique : signification précise des informations échangées préservée et comprise de tous;
- niveau technique : planification des questions techniques relatives à la mise en relation des systèmes et services informatiques.

Le présent chapitre traite de l'interopérabilité sémantique.

L'interopérabilité sémantique entre composantes ou systèmes d'information hétérogènes et dans les systèmes d'échange nécessite de poser un contenu informationnel compréhensible par les différents partenaires.

Les spécifications d'interopérabilité sémantique imposent de définir un langage commun permettant aux applications des systèmes d'information participants d'interpréter de façon homogène la nature et les valeurs des données transmises et de les réutiliser sans erreur ou perte d'information.

Différentes nomenclatures sont ainsi définies pour y répondre.

Ce chapitre décrit l'interopérabilité entre l'ENT et le SI du ministère en charge de l'Éducation nationale. D'autres spécificités peuvent être à prendre en compte pour d'autres systèmes d'information (par exemple, SI du ministère en charge de l'enseignement agricole, ou le SI d'une collectivité territoriale).

Les nomenclatures de la BCN (Base centrale des nomenclatures) constituent un langage commun entre le système d'information de l'Éducation nationale et celui de l'Enseignement supérieur et de la Recherche : nomenclatures et règles de gestion et de contrôle propres, ainsi que certaines nomenclatures interministérielles et internationales.

Elles sont mises à jour régulièrement et historisées au moyen de dates d'ouverture et de fermeture.

Elles sont en consultation sur le site de la [BCN](#)¹²

¹¹ Voir le document principal au chapitre « Qualités attendues de la solution ENT / Interopérabilité »

¹² BCN : base centrale des nomenclatures (<http://infocentre.pleiade.education.fr/bcn/>)

Les nomenclatures sont précisées pour :

- les codes des projets ENT ;
- les modules élémentaires de formation ;
- les enseignements ;
- les nomenclatures académiques transmises par le SI du MEN ;
- les profils de l'accédant ;
- les personnes en relation avec les élèves.

5.2. Codes des projets ENT

Ce chapitre présente la liste des codes identifiant les projets ENT. Chaque projet ENT **DOIT** être identifié par un code unique sur le périmètre national. En effet, la combinaison du code projet ENT avec l'identifiant des utilisateurs permet de garantir au niveau national l'unicité de l'identifiant utilisateur transmis au GAR.

Ce code est donné pour le second degré dans les tableaux ci-après : il est codé sur deux caractères « L » et « C » dont les valeurs sont indiquées aux chapitres 5.2.1 et 5.2.2.

La réforme territoriale de 2015-2016 amène des évolutions aussi bien au niveau du nombre des régions que les départements associés.

Pour les projets ENT déjà en place, les codes déjà utilisés sont conservés, un complément de codification est proposé pour prendre en compte les évolutions de la réforme territoriale.

5.2.1. Codes avant la réforme territoriale

Ces codes ont été attribués aux régions et départements, avant le découpage en 13 régions adopté en 2015-2016. Les projets ENT déjà identifiés avec ces codes conservent leur numérotation.

Porteurs Régions	L	C
Alsace	A	0
Aquitaine	B	0
Auvergne	C	0
Bourgogne	D	0
Bretagne	E	0
Centre	F	0
Champagne-Ardenne	G	0
Corse	H	0
Franche-Comté	I	0
Île-de-France	J	0
Languedoc-Roussillon	K	0

Porteurs Régions	L	C
Limousin	L	0
Lorraine	M	0
Midi-Pyrénées	N	0
Nord-Pas-de-Calais	O	0
Basse-Normandie	P	0
Haute-Normandie	Q	0
Pays de la Loire	R	0
Picardie	S	0
Poitou-Charentes	T	0
Provence-Alpes-Côte-d'Azur	U	0
Rhône-Alpes	V	0

Porteurs Départements	L	C
(01) Ain	V	1
(02) Aisne	S	1
(03) Allier	C	1
(04) Alpes-de-Haute-Provence	U	1
(05) Hautes-Alpes	U	2
(06) Alpes-Maritimes	U	3
(07) Ardèche	V	2
(08) Ardennes	G	1
(09) Ariège	N	1
(10) Aube	G	2
(11) Aude	K	1
(12) Aveyron	N	2
(13) Bouches-du-Rhône	U	4
(14) Calvados	P	1
(15) Cantal	C	2
(16) Charente	T	1
(17) Charente-Maritime	T	2
(18) Cher	F	1
(19) Corrèze	L	1
(2A) Corse-du-Sud	H	1
(2B) Haute-Corse	H	2
(21) Côte-d'Or	D	1
(22) Côtes-d'Armor	E	1
(23) Creuse	L	2
(24) Dordogne	B	1
(25) Doubs	I	1
(26) Drôme	V	3
(27) Eure	Q	1
(28) Eure-et-Loir	F	2
(29) Finistère	E	2
(30) Gard	K	2
(31) Haute-Garonne	N	3
(32) Gers	N	4
(33) Gironde	B	2
(34) Hérault	K	3
(35) Ille-et-Vilaine	E	3
(36) Indre	F	3

Porteurs Départements	L	C
(37) Indre-et-Loire	F	4
(38) Isère	V	4
(39) Jura	I	2
(40) Landes	B	3
(41) Loir-et-Cher	F	5
(42) Loire	V	5
(43) Haute-Loire	C	3
(44) Loire-Atlantique	R	1
(45) Loiret	F	6
(46) Lot	N	5
(47) Lot-et-Garonne	B	4
(48) Lozère	K	4
(49) Maine-et-Loire	R	2
(50) Manche	P	2
(51) Marne	G	3
(52) Haute-Marne	G	4
(53) Mayenne	R	3
(54) Meurthe-et-Moselle	M	1
(55) Meuse	M	2
(56) Morbihan	E	4
(57) Moselle	M	3
(58) Nièvre	D	2
(59) Nord	O	1
(60) Oise	S	2
(61) Orne	P	3
(62) Pas-de-Calais	O	2
(63) Puy-de-Dôme	C	4
(64) Pyrénées-Atlantiques	B	5
(65) Hautes-Pyrénées	N	6
(66) Pyrénées-Orientales	K	5
(67) Bas-Rhin	A	1
(68) Haut-Rhin	A	2
(69) Rhône	V	6
(70) Haute-Saône	I	3
(71) Saône-et-Loire	D	3
(72) Sarthe	R	4
(73) Savoie	V	7
(74) Haute-Savoie	V	8

Porteurs Départements	L	C
(75) Paris	J	1
(76) Seine-Maritime	Q	2
(77) Seine-et-Marne	J	2
(78) Yvelines	J	3
(79) Deux-Sèvres	T	3
(80) Somme	S	3
(81) Tarn	N	7
(82) Tarn-et-Garonne	N	8
(83) Var	U	5
(84) Vaucluse	U	6
(85) Vendée	R	6
(86) Vienne	T	4
(87) Haute-Vienne	L	3
(88) Vosges	M	4
(89) Yonne	D	4
(90) Territoire de Belfort	I	4
(91) Essonne	J	4
(92) Hauts-de-Seine	J	5
(93) Seine-Saint-Denis	J	6
(94) Val-de-Marne	J	7
(95) Val-d'Oise	J	8
(971) Guadeloupe	W	1
(972) Martinique	W	2
(973) Guyane	W	3
(974) La Réunion	W	4
(975) Saint-Pierre-et-Miquelon	W	5
(976) Mayotte	W	6
(984) Terres Australes et Antarctiques	W	7
(986) Wallis et Futuna	W	8
(987) Polynésie Française	W	9
(988) Nouvelle-Calédonie	X	1

5.2.2. Codes après la réforme territoriale

Les régions ou départements porteurs de projet ENT sont depuis 2016 identifiés par les lettres L C dont les valeurs figurent dans les tableaux ci-après.

Les académies porteuses de projet seront identifiées par les codes correspondant à la région ou au DOM lorsque les territoires se superposent, ou avec un code spécifique sinon (cas des régions pluri-académiques).

Porteurs Régions	L	C
Auvergne-Rhône-Alpes	C	0
Bourgogne-Franche-Comté	D	0
Bretagne	E	0
Centre-Val de Loire	F	0
Corse	H	0
Grand Est	A	0
Hauts de France	O	0
Île-de-France	J	0
Normandie	P	0
Nouvelle-Aquitaine	B	0
Occitanie	K	0
Pays de la Loire	R	0
Provence-Alpes-Côte d'Azur	U	0

Porteurs départements	L	C
(01) Ain	C	5
(02) Aisne	O	3
(03) Allier	C	1
(04) Alpes-de-Haute-Provence	U	1
(05) Hautes-Alpes	U	2
(06) Alpes-Maritimes	U	3
(07) Ardèche	C	6
(08) Ardennes	A	3
(09) Ariège	K	6
(10) Aube	A	4
(11) Aude	K	1
(12) Aveyron	K	7
(13) Bouches-du-Rhône	U	4
(14) Calvados	P	1
(15) Cantal	C	2
(16) Charente	B	6
(17) Charente-Maritime	B	7
(18) Cher	F	1
(19) Corrèze	B	8
(21) Côte-d'Or	D	1
(22) Côtes-d'Armor	E	1
(23) Creuse	B	9
(24) Dordogne	B	1
(25) Doubs	D	5
(26) Drôme	C	7
(27) Eure	P	4
(28) Eure-et-Loir	F	2
(29) Finistère	E	2
(2A) Corse-du-Sud	H	1
(2B) Haute-Corse	H	2
(30) Gard	K	2
(31) Haute-Garonne	K	8
(32) Gers	K	9
(33) Gironde	B	2
(34) Hérault	K	3
(35) Ille-et-Vilaine	E	3
(36) Indre	F	3

Porteurs départements	L	C
(37) Indre-et-Loire	F	4
(38) Isère	C	8
(39) Jura	D	6
(40) Landes	B	3
(41) Loir-et-Cher	F	5
(42) Loire	C	9
(43) Haute-Loire	C	3
(44) Loire-Atlantique	R	1
(45) Loiret	F	6
(46) Lot	K	A
(47) Lot-et-Garonne	B	4
(48) Lozère	K	4
(49) Maine-et-Loire	R	2
(50) Manche	P	2
(51) Marne	A	5
(52) Haute-Marne	A	6
(53) Mayenne	R	3
(54) Meurthe-et-Moselle	A	7
(55) Meuse	A	8
(56) Morbihan	E	4
(57) Moselle	A	9
(58) Nièvre	D	2
(59) Nord	O	1
(60) Oise	O	4
(61) Orne	P	3
(62) Pas-de-Calais	O	2
(63) Puy-de-Dôme	C	4
(64) Pyrénées-Atlantiques	B	5
(65) Hautes-Pyrénées	K	5
(66) Pyrénées-Orientales	K	B
(67) Bas-Rhin	A	1
(68) Haut-Rhin	A	2
(69) Rhône	C	A
(70) Haute-Saône	D	7
(71) Saône-et-Loire	D	3
(72) Sarthe	R	4
(73) Savoie	C	B

Porteurs départements	L	C
(74) Haute-Savoie	C	C
(75) Paris	J	1
(76) Seine-Maritime	P	5
(77) Seine-et-Marne	J	2
(78) Yvelines	J	3
(79) Deux-Sèvres	B	A
(80) Somme	O	5
(81) Tarn	K	C
(82) Tarn-et-Garonne	K	D
(83) Var	U	5
(84) Vaucluse	U	6
(85) Vendée	R	5
(86) Vienne	B	B
(87) Haute-Vienne	B	C
(88) Vosges	A	A
(89) Yonne	D	4
(90) Territoire de Belfort	D	8
(91) Essonne	J	4
(92) Hauts-de-Seine	J	5
(93) Seine-Saint-Denis	J	6
(94) Val-de-Marne	J	7
(95) Val-d'Oise	J	8
(971) Guadeloupe	W	1
(972) Martinique	W	2
(973) Guyane	W	3
(974) La Réunion	W	4
(975) Saint-Pierre-et-Miquelon	W	5
(976) Mayotte	W	6
(984) Terres Australes et Antarctiques	W	7
(986) Wallis et Futuna	W	8
(987) Polynésie Française	W	9

Porteurs Académie	L	C
Aix-Marseille	U	7
Amiens	O	6
Besançon	D	9
Bordeaux	B	D
Caen	P	6
Clermont-Ferrand	C	D
Corse	H	0
Créteil	J	9
Dijon	D	A
Grenoble	C	E
Lille	O	7
Limoges	B	E
Lyon	C	F
Montpellier	K	E
Nancy-Metz	A	B
Nantes	R	0
Nice	U	8
Orléans-Tours	F	0
Paris	J	A
Poitiers	B	F
Reims	A	C
Rennes	E	0
Rouen	P	7
Strasbourg	A	D
Toulouse	K	F
Versailles	J	B
Guadeloupe	W	1
Guyane	W	3
La Réunion	W	4
Martinique	W	2

5.3. Regroupement d'écoles ou d'établissements : RPI, cités scolaires

5.3.1. RPI (regroupements pédagogiques intercommunaux)

Les regroupements pédagogiques intercommunaux (RPI) permettent à plusieurs communes, notamment en milieu rural, de se réunir pour l'établissement et l'entretien d'une école :

- dans les RPI dits « dispersés », chaque école rassemble les élèves de plusieurs communes par niveau pédagogique et garde son statut juridique et sa direction d'école ;
- dans le cas de RPI dits « concentrés », l'ensemble des élèves des communes concernées est scolarisé dans l'école de l'une des communes.

Les configurations de RPI peuvent se retrouver dans la base RAMSESE¹³ au travers de la table qui liste les zones et de la table qui fait le lien entre les zones et les établissements. Dans les exports ENT, les écoles appartenant à un RPI peuvent être identifiées par l'intermédiaire du champ « ENTEcoleRPI » qui indique le code du RPI, son nom et le code département associé.

Les solutions ENT peuvent donc se baser sur cette information pour reconstituer les RPI du projet ENT.

5.3.2. Cités scolaires

Une cité scolaire publique est un ensemble immobilier constitué d'au moins 2 établissements scolaires publics qui utilisent en commun des locaux, et dont au moins un est un établissement du second degré. On entend ici par établissement les EPLE (établissements publics locaux d'enseignement), soit collège, lycée, lycée professionnel, et les écoles communales du premier degré.

Une cité scolaire privée est un ensemble immobilier constitué d'au moins 2 structures ayant un type d'UAI différent parmi les types d'UAI suivants : lycée, lycée professionnel, collège ou école ordinaire du premier degré. Dans la base RAMSESE, la cité scolaire est traitée comme une zone à laquelle on peut rattacher la liste des UAI faisant partie d'une même cité scolaire, sachant que seuls doivent être rattachés à la cité scolaire les établissements juridiquement autonomes.

Dans les exports ENT, les établissements au sein d'une cité scolaire sont identifiés par le champ « ENTétablissementStructRattachFct1 » qui contient l'identifiant de l'établissement responsable de gestion de la cité scolaire à laquelle appartient éventuellement l'établissement si celui-ci fait partie du périmètre du projet ENT.

Les solutions ENT peuvent donc se baser sur cette information pour reconstituer la notion de cité scolaire.

¹³ RAMSESE : (répertoire académique et ministériel sur les établissements du système éducatif)

5.4. Nomenclatures des MEF

5.4.1. Généralités

La formation que suit un élève pendant une année scolaire est qualifiée par différentes nomenclatures qui s'articulent autour des MEF (Modules élémentaires de formation). Chaque nomenclature apporte un niveau plus ou moins fin d'information. Ces nomenclatures sont organisées selon deux axes hiérarchisés (détaillés dans les chapitres suivants) :

- la thématique de la formation ;
- la position de la formation par rapport à un cursus.

La **thématique de la formation**, dont les nomenclatures associées sont les suivantes :

Nom nomenclature	Codification dans la BCN
MEF	<i>N_MEF</i>
Dispositif de formation	<i>N_DISPOSITIF_FORMATION</i>
Spécialité de formation du diplôme	<i>N_FORMATION_DIPLOME</i>
Durée	<i>N_DUREE_DISPOSITIF</i>
Année	<i>N_ANNEE_DISPOSITIF</i>
Type MEF	<i>N_TYPE_MEF</i>

Tableau 10 : Nomenclatures associées à la thématique de la formation

La spécialité de formation du diplôme est construite comme illustré Figure 17 à partir des nomenclatures suivantes :

- catégorie (*N_CATEGORIE_SPECIALITE*) ;
- domaine (*N_DOMAINE_SPECIALITE*) ;
- groupe (*N_GROUPE_SPECIALITE*) ;
- numéro d'ordre.



Figure 17 : Nomenclature de la spécialité de formation du diplôme

La nomenclature *N_GROUPE_SPECIALITE* est définie par le Conseil national de l'information statistique (CNIS).

Nota : le niveau de formation du diplôme (*N_NIVEAU_FORMATION_DIPLOME*) peut être déterminé à partir du dispositif de formation (*N_DISPOSITIF_FORMATION*). La spécialité du diplôme (*N_FORMATION_DIPLOME*) et le niveau de formation du diplôme sont liés.

Un exemple est proposé au chapitre 5.4.4 « Synthèse des informations disponibles à partir d'un MEF national ».

La **position de la formation par rapport à un cursus**, dont les nomenclatures associées sont les suivantes :

Nom nomenclature	Codification dans la BCN
MEFSTAT11	V_MEF_STAT_11
MEFSTAT9	N_MEF_STAT_9
MEFSTAT8	N_MEF_STAT_8
MEFSTAT7	N_MEF_STAT_7
MEFSTAT6	N_MEF_STAT_6
MEFSTAT5	N_MEF_STAT_5
MEFSTAT4	N_MEF_STAT_4
MEFSTAT3	N_MEF_STAT_3
MEFSTAT2	N_MEF_STAT_2
MEFSTAT1	N_MEF_STAT_1

Tableau 11 : Nomenclatures associées à la position de la formation dans le cursus

5.4.2. Thématique de la formation

5.4.2.1. MEF nationaux et MEF académiques

Il existe deux catégories de MEF codifiant la thématique de formation : les MEF nationaux et les MEF académiques. Ces deux types de MEF sont codifiés sur 11 caractères.

Les **MEF nationaux** ont une portée nationale. Le 11^e et dernier caractère d'un MEF national vaut toujours « 0 » (zéro). Les MEF nationaux sont codés sur 10 caractères dans la BCN et sur 11 caractères lors de transmission dans le SI du MEN.

Les **MEF académiques** sont des MEF créés localement, en respectant certaines règles de gestion, pour répondre aux besoins suivants :

- la mise en place de formations nationales à gestion académique, telles que les sections linguistiques, sportives, les formations qualifiantes de SEGPA, certaines actions de la MGI (Mission générale d'insertion) ;
- les besoins propres de l'académie : mise en place pour des publics ciblés de formations ayant une durée ou une spécialité particulière (par exemple, préparation d'un bac technologique en 3 ans au lieu de 2).

Le 11^e et dernier caractère d'un MEF académique est un chiffre différent de « 0 » (zéro) ou bien une lettre (cf. nomenclature N_TYPE_MEF).

Les académies peuvent adapter la durée du dispositif de formation ou la spécialité. Dans le 2^e cas, le 8^e caractère du MEF devient une lettre.

Lorsqu'un MEF académique est créé, il est associé à un **MEF de rattachement**. Il s'agit du MEF national à partir duquel le MEF académique a été « profilé ».

Les MEF des formations de l'enseignement agricole, proposées en voie initiale (scolaire), sont également disponibles dans la BCN et intégrés dans les fichiers d'alimentation des ENT.

5.4.2.2. Enseignements

Une thématique de formation définie par un MEF correspond à un ensemble d'**enseignements** ou matières enseignées (cf. chapitre 0). Les correspondances sont définies dans la table *N_MEF_MATIERE* de la BCN.

Nota : Certains MEF nationaux n'ont pas de définition de programme dans *N_MEF_MATIERE*.

5.4.2.3. Codification

La codification de la thématique de formation d'un MEF est illustrée Figure 18 et Figure 19. Deux exemples de MEF sont également présentés : « 1CAP2 CHOCOLATIER CONFISEUR » et « PREMIERE SCIENTIFIQUE SVT ».

Cette codification n'est valable que pour les MEF nationaux.

3 caractères			5 caractères					1 caractère	1 caractère	1 caractère
MEF (N_MEF)										
Dispositif de formation (N_DISPOSITIF_FORMATION)			Spécialité (N_FORMATION_DIPLOME)					Durée (N_DUREE_DISPOSITIF)	Année (N_ANNEE_DISPOSITIF)	Type MEF (N_TYPE_MEF)
			Catégorie (N_CATEGORIE_SPECIALITE)							
			Domaine (N_DOMAINE_SPECIALITE)							
			Groupe (N_GROUPE_SPECIALITE)							
						N° d'ordre				

2		4		1	2		2	1	3	3	2		1	0
1CAP2 CHOCOLATIER CONFISEUR														
CAP EN 2 ANS				CHOCOLATIER CONFISEUR							DEUX ANS		PREMIERE ANNEE DU DISPO.DE FORMATION	MEF NATIONAL
				SPECIALITE TECHNICO-PROF DE PRODUCTION										
				TRANSFORMATIONS										
				AGRO-ALIMENTAIRE, ALIMENTATION, CUISINE										
									33					

Figure 18 : Nomenclature des MEF nationaux pour le MEF « 1CAP2 CHOCOLATIER CONFISEUR »

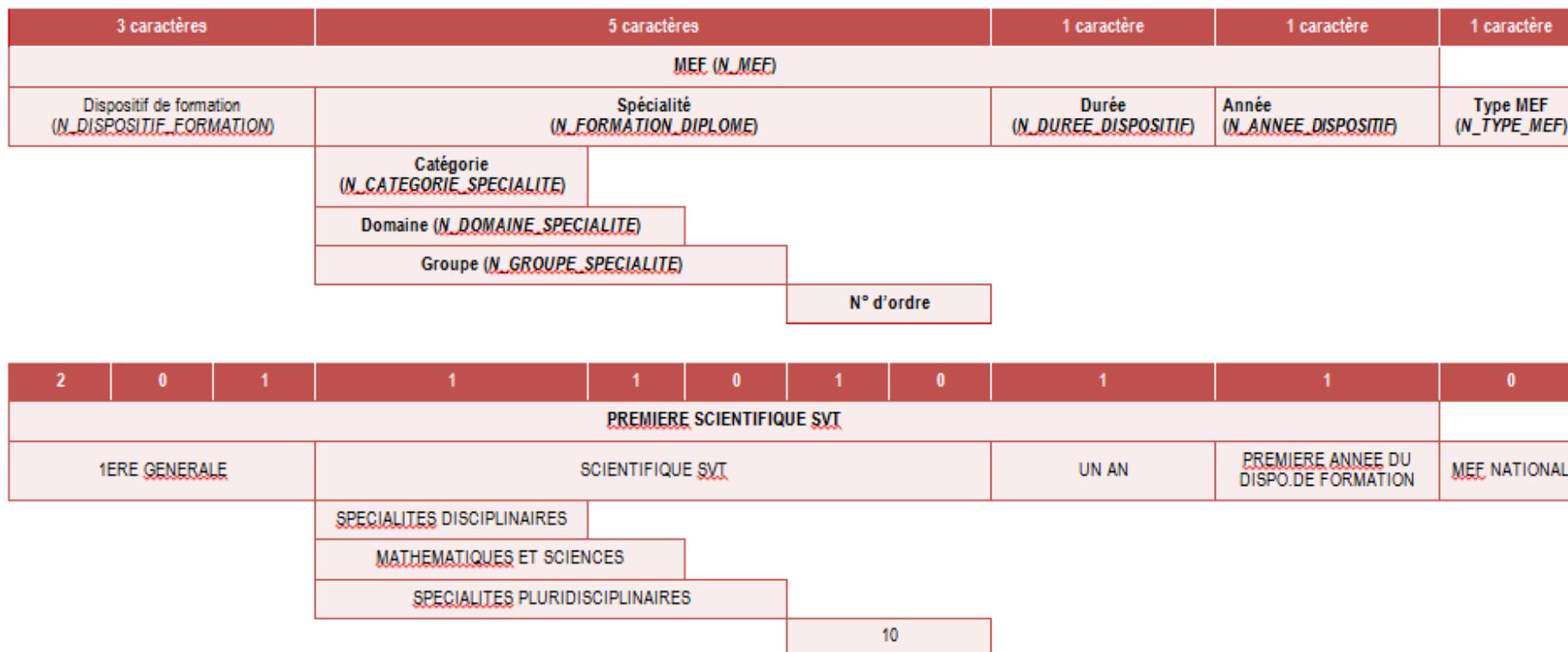


Figure 19 : Nomenclature des MEF nationaux pour le MEF « PREMIERE SCIENTIFIQUE SVT »

5.4.3. Classification de la formation par rapport à un CURSUS

À chaque MEF national est associé un unique MEFSTAT11.

Le MEFSTAT11 est un **code hiérarchisé** : plus on lit de caractères, plus la formation est décrite finement et plus on précise la classification de la formation par rapport au cursus.

9 nomenclatures, MEF_STAT_1 à MEF_STAT_9, permettent de lire chacun **des niveaux de rupture**.

Rupture	Niveau d'information	Exemple
Au 1er caractère	Degré d'enseignement	1er degré, 2nd degré, post-Bac...
Au 2ème caractère	Cycle d'enseignement	1er cycle du 2nd degré, 2nd cycle pro, 2nd cycle Général & Technologique...
Au 3ème caractère	Dispositif de formation	CAP en 1 an, CAP en 2ans, ..., BTS en 2 ans, ...
Au 4ème caractère	Classe	6ème, 5ème, ..., 2nde Pro, ..., 1ère Général & Technologique, ...
Au 5ème caractère	Filière du 2nd cycle Général & Technologique	Voie Générale / Voie Technologique / BT
Au 6ème caractère	Série du bac G & T ou Type de CPGE	S, L, ES, STI, STL, ... ou Scientifique, Littéraire, Eco & Commerciales
Au 7ème caractère	Catégorie de Spécialités	Nomenclature CNIS en 4 postes
Au 8ème caractère	Domaine de Spécialités	Nomenclature CNIS en 17 postes
Au 9ème caractère	Groupe de Spécialités	Nomenclature CNIS en 93 postes

Tableau 12 : Niveaux de rupture du MEFSTAT11

La classification d'une formation par rapport à un cursus est illustrée Figure 20 et Figure 21 avec deux exemples de MEF / MEFSTAT11 présentés : « 1CAP2 CHOCOLATIER CONFISEUR » et « PREMIERE SCIENTIFIQUE SVT ».

11 caractères										
MEFSTAT11 (V_MEF_STAT_11)										
MEFSTAT9 (N_MEF_STAT_9)										
MEFSTAT8 (N_MEF_STAT_8)										
MEFSTAT7 (N_MEF_STAT_7)										
MEFSTAT6 (N_MEF_STAT_6)										
MEFSTAT5 (N_MEF_STAT_5)										
MEFSTAT4 (N_MEF_STAT_4)										
MEFSTAT3 (N_MEF_STAT_3)										
MEFSTAT2 (N_MEF_STAT_2)										
MEFSTAT1 (N_MEF_STAT_1)										
2	3	2	1	0	0	2	2	1	3	3
1CAP2 CHOCOLATIER CONFISEUR										
1CAP2 G221 : AGRO-ALIMENTAIRE, CUISINE										
1CAP2 DO22 : TRANSFORMATIONS										
1CAP2 DOMAINES DE LA PRODUCTION										
CAP EN 2 ANS : 1ERE ANNEE										
CAP EN 2 ANS : 1ERE ANNEE										
CAP EN 2 ANS : 1ERE ANNEE										
CAP EN 2 ANS										
2D CYCLE PROFESSIONNEL										
2ND DEGRE										

Figure 20 : Nomenclature des MEFSTAT nationaux pour le MEF « 1CAP2 CHOCOLATIER CONFISEUR »

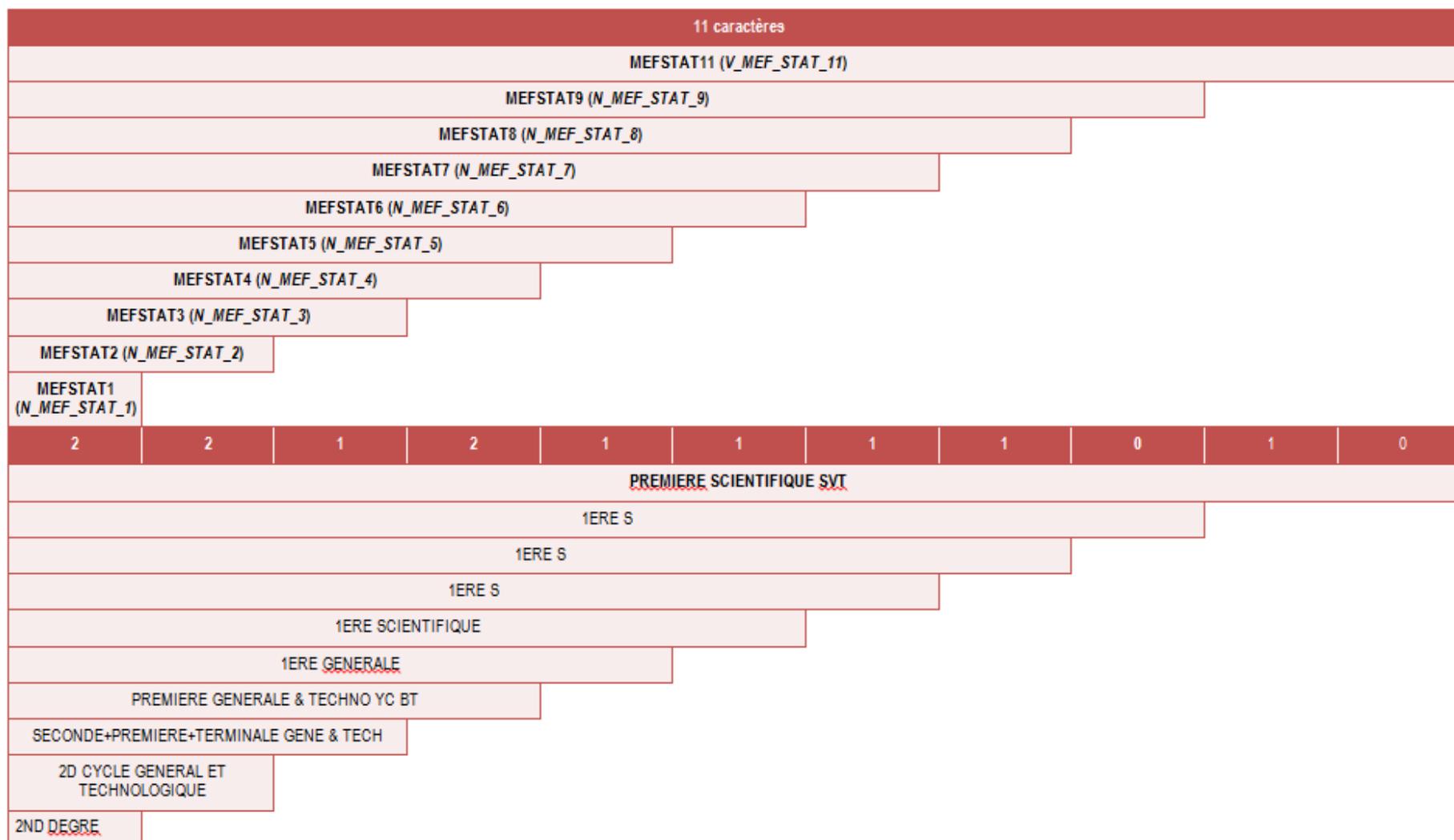


Figure 21 : Nomenclature des MEFSTAT nationaux pour le MEF « PREMIERE SCIENTIFIQUE SVT »

5.4.4. Synthèse des informations disponibles à partir d'un MEF national

Nomenclature	Code exemple 1	Libellé exemple 1	Code exemple 2	Libellé exemple 2	Code exemple 3	Libellé exemple 3
N_MEF	2412213321	1CAP2 CHOCOLATIER CONFISEUR	2011101011	PREMIERE SCIENTIFIQUE SVT	1021000111	4EME
DISPOSITIF_FORMATI ON	241	CAP EN 2 ANS	201	1ERE GENERALE	102	4EME
N_NIVEAU_FORMATI ON_ DIPLOME issu de la table N_DISPOSITIF_FORMA TION	500	CERTIFICAT D'APTITUDES PROFESSION- NELLES	470	BAC GENERAL	670	FORMATIONS GENERALES DE 1ER CYCLE
N_FORMATION_DIPL OME	(500)22133	CHOCOLATIER CONFISEUR	(470)11010	SCIENTIFIQUE SVT	(670)10001	GENERAL
V_MEF_STAT_11 issu de la table N_DISPOSITIF_FORMA TION	23210022133	1CAP2 CHOCOLATIER CONFISEUR	22121111010	PREMIERE SCIENTIFIQUE SVT	21150010001	4EME
N_MEF_STAT_9	232100221	1CAP2 G221 : AGRO- ALIMENTAIRE, CUISINE	221211110	1ERE S	211500100	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_8	23210022	1CAP2 DO22 : TRANSFORMATIO NS	22121111	1ERE S	21150010	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_7	2321002	1CAP2 DOMAINE DE LA PRODUCTION	2212111	1ERE S	2115001	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_6	232100	CAP EN 2 ANS : 1ERE ANNEE	221211	1ERE SCIENTIFIQUE	211500	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_5	23210	CAP EN 2 ANS : 1ERE ANNEE	22121	1ERE GENERALE	21150	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_4	2321	CAP EN 2 ANS : 1ERE ANNEE	2212	PREMIERE GENERALE & TECHNO YC BT	2115	4EME GENERALE (N.C 4E AES)
N_MEF_STAT_3	232	CAP EN 2 ANS	221	SECONDE+PREMI ERE+TERMINALE GENE & TECH	211	6EME A 3EME + 3E D'INSERTION
N_MEF_STAT_2	23	2D CYCLE PROFESSIONNEL	22	2D CYCLE GENERAL ET TECHNOLOGIQUE	21	1ER CYCLE
N_MEF_STAT_1	2	2ND DEGRE	2	2ND DEGRE	2	2ND DEGRE

Tableau 13 : Exemples d'informations disponibles à partir d'un MEF national

5.5. Enseignements, disciplines et niveaux des formations

5.5.1. Nomenclatures « de gestion » utilisées par le MEN

Les nomenclatures utilisées par le ministère sont décrites dans la BCN.

5.5.1.1. Enseignements

Une formation comprend des **enseignements** (ou matières enseignées), qui sont codés sur 6 caractères :

- les 2 premiers caractères codent les **familles de matières** (Langues vivantes, Sciences...);
- les 4 premiers caractères codent les **matières** (Allemand, Mathématiques...);
- le 5^e caractère code les **modalités d'éloignement** (enseignement dans l'établissement, par correspondance...);
- le 6^e caractère code les **modalités d'enseignement** (une option prise en premier ou second choix...).

La codification des enseignements est illustrée Figure 22 avec un exemple d'enseignement : « ALLEMAND LV1 ».

2 caractères		2 caractères		1 caractère		1 caractère	
Enseignement <i>(N_MATIERE_ENSEIGNEE)</i>							
Matière <i>(N_MATIERE)</i>				Modalité d'éloignement <i>(N_MODALITE_ELOIGNEMENT)</i>		Modalité d'enseignement <i>(N_MODALITE_ENSEIGNEMENT)</i>	
Famille de matières <i>(N_FAMILLE_MATIERE)</i>							
0	3	0	1	0			1
ALLEMAND LV1							
ALLEMAND				ENSEIGNEMENT DANS L'ETABLISSEMENT		OPTION CHOISIE EN PREMIER	
LANGUES VIVANTES							

Figure 22 : Nomenclature des matières enseignées pour l'enseignement « ALLEMAND LV1 »

5.5.1.2. Disciplines

Pour un enseignant, il convient de distinguer sa discipline de recrutement de sa discipline de poste :

- **discipline de recrutement** : discipline correspondant au concours que le candidat a passé pour être recruté ;
- **discipline de poste** : il s'agit de la discipline effectivement enseignée. Cette information est renseignée par le service chargé de la gestion des personnels enseignants de l'enseignement scolaire du MEN en fonction des matières enseignées. Elle peut correspondre à plusieurs disciplines de recrutement (et donc plusieurs concours).

Disciplines de recrutement	Discipline de poste associée
0201A LETTRES CLASSIQUES	L0201 LETTRES CLASSIQUES
0201B GRAMMAIRE	L0201 LETTRES CLASSIQUES
0201E LETTRES CLASSIQUES	L0201 LETTRES CLASSIQUES

Tableau 14 : Exemples de disciplines de recrutement et de disciplines de postes associées

La codification des disciplines de poste est illustrée. Un exemple de discipline de poste est également présenté : « ALLEMAND LETTRES ».

1 caractère	2 caractères	2 caractères
Discipline de poste (N_DISCIPLINE_POSTE)		
Type de poste (N_TYPE_POSTE)	Discipline de compétence (N_DISCIPLINE_COMPETENCE)	
	Pivot discipline (N_PIVOT_DISCIPLINE)	

L	0	4	5	1
ALLEMAND LETTRES				
ENSEIGNEMENT EN LYCEE	ALLEMAND LETTRES			
	LANGUES VIVANTES			

Figure 23 : Nomenclature des disciplines pour la discipline de poste « ALLEMAND LETTRES »

5.5.2. Correspondances BCN / ScoLOMFR

Les solutions ENT reposent sur des annuaires alimentés par les données du SI du ministère en charge de l'Éducation nationale :

- les attributs de l'annuaire ENT sont définies dans l'annexe Annuaire ;
- les attributs alimentés par le SI du MEN sont repris dans l'annexe Annuaire ;
- la référence des nomenclatures est la Base centrale des nomenclatures (BCN)¹⁴.

¹⁴ BCN (<http://infocentre.pleiade.education.fr/bcn/>)

Parmi les données qui peuvent être transmises par la solution ENT aux services Tiers, des informations sur l'accédant, non associées à une identité, permettent d'assurer l'authentification, le contrôle d'accès au service et la fourniture du service.

Certains attributs, décrits selon la nomenclature BCN, ne peuvent être facilement exploités par les services Tiers fournisseurs de contenus pédagogiques, organisés selon une approche plus pédagogique qu'administrative.

Afin d'articuler les deux approches, un travail de mise en correspondance est réalisé, sur la base du profil ScoLOMFR¹⁵ pour les informations « Niveaux » et « Domaines d'enseignement ».

ScoLOMFR fournit un vocabulaire spécifique d'alignement ScoLOMFR-BCN, qui définit les équivalences. Il est fourni au format SKOS¹⁶.

Les équivalences sont décomposées en alignement exact, alignement proche, alignement générique et alignement spécifique.

Le profil ScoLOMFR est évolutif (avec un comité de pilotage annuel prenant en compte les demandes d'évolution et une mise à jour annuelle publiée en septembre). La date de publication de la version 4.0.0 dans son intégralité est prévue le 14 mai 2018.

Les [vocabulaires](#) sont consultables en ligne¹⁷. Un [manuel technique](#)¹⁸ est également disponible.

5.5.2.1. Niveaux

Les niveaux détaillés ScoLOMFR Voc-022 sont mis en correspondance avec le code MEFSTAT fourni aux ENT par le SI MEN.

Dans le premier degré, l'attribut ENTEleveNiveau (classe ENTEleve) est renseigné à partir de la nomenclature BCN N_MEFSTAT_4.

Dans le second degré, l'attribut ENTMEFSTAT11 est alimenté par le SI du MEN avec la nomenclature BCN V_MEFSTAT_11 (c'est-à-dire encodée sur 11 caractères). Le niveau détaillé de la liste ScoLOMFR Voc-022 correspond à un nombre variable de caractères du MEFSTAT11 : généralement les 6 premiers caractères de cet attribut correspondant à la nomenclature BCN N_MEFSTAT_6 sont utilisés dans la liste ScolomFR Voc-022.

5.5.2.2. Domaines d'enseignement

Les domaines d'enseignement ScoLOMFR Voc-015 sont mis en correspondance avec la nomenclature BCN N_MATIERE_ENSEIGNEE.

Dans le second degré, les attributs ENTAuxEnsMatiereEnseignEtab, ENTAuxEnsClassesMatiere, ENTAuxEnsGroupesMatiere, (classe auxiliaire ENTAuxEnseignant) sont renseignés à partir de la nomenclature BCN N_MATIERE_ENSEIGNEE.

¹⁵ ScoLOMFR (<https://www.reseau-canope.fr/scolomfr/>)

¹⁶ SKOS (Simple Knowledge Organisation System) - (<http://www.sparna.fr/skos/SKOS-traduction-francais.html>)

¹⁷ Vocabulaires ScoLOMFR (<https://www.reseau-canope.fr/scolomfr/telecharger.html>)

¹⁸ Manuel technique ScoLOMFR (<https://www.reseau-canope.fr/scolomfr/se-documenter.html>)

5.5.3. Correspondances BCN / nomenclatures de l'enseignement agricole

Le système d'information de l'enseignement agricole s'appuie sur des nomenclatures propres. Pour faciliter les échanges de données, entre le ministère en charge de l'enseignement agricole et le ministère en charge de l'Éducation nationale ou services Tiers, une correspondance a été établie entre les nomenclatures de référence de l'enseignement agricole et celles contenues dans la BCN, sauf pour celles utilisées dans la gestion des ressources humaines et celle décrivant les matières enseignées.

Les nomenclatures spécifiques aux besoins de gestion des ressources humaines à l'Éducation nationale ne peuvent correspondre avec les nomenclatures de l'enseignement agricole. Il est alors nécessaire d'utiliser une table de référence spécifique aux besoins de l'enseignement agricole.

Ainsi, l'attribut ENTPersonFonctions (classe auxiliaire ENTAuxEnseignant) est renseigné pour l'enseignement agricole à partir des nomenclatures N_FONCTION_FILIERE et N_FAMILLE_POSTE_EA (table contenant les familles de postes de l'enseignement agricole) Cette table est disponible dans la BCN.

Exemples de valeurs du champ ENTPersonFonctions pour les enseignants, fourni par le SI de l'enseignement agricole :

- 9801030000000\$ENS\$ENSEIGNEMENT DEVANT ELEVES\$FD0032\$Aménagement/Aménag Paysagers
- 9801034000000\$ENS\$ENSEIGNEMENT DEVANT ELEVES\$FD0001\$MATHÉMATIQUES
- 9801022000000\$ENS\$ENSEIGNEMENT DEVANT ELEVES\$FD0046\$ZOOTECNIE/HIPPOLOGIE
- 9801034000000\$ENS\$ENSEIGNEMENT DEVANT ELEVES\$LV01\$Anglais

Exemples de valeurs du champ ENTPersonFonctions pour d'autres fonctions :

- 9801012000000\$ADM\$FONCTION ADMINISTRATIVE\$FS0019\$Administratif cat. B
- 9801014000000\$EDU\$EDUCATION\$FS0011\$CPE
- 9801014000000\$LAB\$PERSONNELS DE LABORATOIRE\$FS0015\$Laboratoire cat. B
- 9801014000000\$MDS\$PERSONNELS MEDICO-SOCIAUX\$FS0017\$Santé
- 9801014000000\$TEC\$PERSONNELS TECHNIQUES\$FS0022\$Surveillance cat. B
- 9801019000000\$DIR\$DIRECTION\$FS0008\$Directeur CFPPA

Pour plus de détails, se reporter à l'annexe 4bis « Alimentation de l'annuaire ENT depuis le SI du ministère en charge de l'Éducation nationale et d'autres SI externes » de l'ensemble annuaire.

5.6. Informations de scolarité transmises par le SI du MEN

Les tableaux ci-dessous reprennent les informations liées aux MEF et aux enseignements qui sont transmises par le SI du MEN au travers des fichiers d'alimentation des annuaires ENT.

5.6.1. Nomenclatures académiques transmises dans le second degré par le biais de l'annuaire académique fédérateur (AAF)

Dans le second degré, deux fichiers contenant des nomenclatures sont transmis par l'AAF aux solutions ENT.

Un premier fichier contient pour chaque Mef :

- le libellé du Mef ;
- le Mef national de rattachement ;
- le code Mef_stat_11.

Un deuxième fichier contient pour chaque code matière le libellé associé.

5.6.2. Informations transmises pour les élèves du second degré

Attribut	Commentaire	Obl/Fac	Mo/Mu	Libellé	Nomenclature	Exemple
MEF	Code du MEF national ou académique	Obl	Mo	ENTEleveMEF	<i>N_MEF (code MEF) + N_TYPE_MEF (code type MEF) [10+1 caractères]</i>	10310019110
Libellé MEF	Libellé du MEF national ou académique	Obl	Mo	ENTEleveLibelleMEF	<i>N_MEF correspondant aux 10 premiers caractères pour les MEF nationaux, texte libre pour les MEF académiques</i>	3EME
Niveau de formation ¹	1ère générale et technologique, 1ère année de CAP en 2 ans...	Obl	Mo	ENTEleveNivFormation	<i>N_MEF_STAT_4</i>	3EME GENERALE
Filière	1ère générale, 1ère année de CAP en 2 ans	Obl	Mo	ENTEleveFiliere	<i>N_MEF_STAT_5</i>	3EME GENERALE
Code des Enseignements	Ensemble des codes des enseignements (=matières) suivis par l'élève (obligatoires, optionnels et de spécialité): Histoire-géographie, Latin, SVT...	Obl	Mu	ENTEleveCodeEnseignements	<i>N_MATIERE_ENSEIGNEE</i>	020700 062900
Établissement de rattachement administratif	Pointeur sur l'établissement principal de l'élève	Obl	Mo	ENTPersonStructRattach		50245

¹ Les valeurs du niveau de formation et de la filière sont basées sur le MEF de rattachement (chaque MEF est associé à un MEF de rattachement et à un MEFSTAT).

Attribut	Commentaire	Obl/Fac	Mo/Mu	Libellé	Nomenclature	Exemple
Établissements et classe associée	Divisions structurelles dans lesquelles est inscrit l'élève (p. ex. 3eB de l'Etab1)	Obl	Mu	ENTEleveClasses	Code de la classe (chaque établissement peut définir sa propre nomenclature)	50245\$TTIE2
Établissements et groupes associés	Groupes d'enseignement auxquels appartient l'élève	Fac	Mu	ENTEleveGroupes	Code du groupe (chaque établissement peut définir sa propre nomenclature)	50245\$TTIE2_A
Date d'entrée dans l'établissement	Date d'entrée dans la (les) division(s) de l'établissement de rattachement administratif courant	Fac	Mu	ENTEleveDateEntreeClasses		50745\$01/09/2019\$2BEP1
Date de sortie de l'établissement	Date de sortie de la (des) division(s) de l'établissement de rattachement administratif courant	Fac	Mu	ENTEleveDateSortieClasses		50745\$01/07/2020\$2BEP1

Tableau 15 : Nomenclatures transmises pour les élèves dans le second degré

5.6.3. Informations transmises pour les enseignants de l'Éducation nationale du second degré

Attribut	Commentaire	Obl/Fac	Mo/Mu	Libellé	Nomenclature	Exemple
Code MEF et libellé associé par établissement	Indique le ou les MEF (académiques ou nationaux) des classes ou groupes de l'enseignant pour chaque établissement	Fac	Mu	ENTAuxEnsMEF	Code MEF : N_MEF (code MEF) + N_TYPE_MEF (code type MEF) [10+1 caractères] Libellé MEF : N_MEF	6709\$10010012110\$6EME 6709\$10110001110\$5EME 6709\$10210001110\$4EME 6709\$10310019110\$3EME
Fonctions	Fonctions multiples (et disciplines associées) dans des établissements, des structures de rattachement fonctionnel (cités scolaires, GRETA, lycée) ou des bassins de formation : responsable ENT, webmestre, responsable sécurité...	Fac	Mu	ENTPersonFonctions	N_FONCTION_FILIERE (code) + N_FONCTION_FILIERE (libellé) + N_DISCIPLINE_POSTE (code) + N_DISCIPLINE_POSTE (libellé)	6709\$ENS\$ENSEIGNEMENT \$L1600\$SCIENCES DE LA VIE ET DE LA TERRE
Catégories de discipline de poste	Physique et électricité appliquée (catégorie : Physique - Chimie)	Fac	Mu	ENTAuxEnsCategoDiscipline	N_PIVOT_DISCIPLINE (code) (code) + N_PIVOT_DISCIPLINE (libellé)	16\$BIOLOGIE - GEOLOGIE
Établissements et matières enseignées associées	Matières multiples enseignées effectivement dans des établissements multiples	Fac	Mu	ENTAuxEnsMatiereEnseignEtab	N_MATIERE_ENSEIGNEE	6709\$SCIENCES DE LA VIE ET DE LA TERRE
Lien Établissement/ Divisions / matières enseignées dans division	Lien Établissement/ Divisions / codes matières enseignées dans division	Fac	Mu	ENTAuxEnsClassesMatiere	N_MATIERE_ENSEIGNEE	6709\$301\$062900 6709\$302\$062900 6709\$401\$062900 ...

Attribut	Commentaire	Obl/Fac	Mo/Mu	Libellé	Nomenclature	Exemple
Lien Établissement/ Groupes /matières enseignées dans groupe	Lien Établissement/ Groupes / codes matières enseignées dans groupe	Fac	Mu	ENTAuxEnsGroupesMatières	N_MATIERE_ENSEIGNEE	6709\$6A\$062900

Tableau 16 : Nomenclatures transmises pour les enseignants de l'Éducation nationale dans le second degré

5.7. Profils de l'accédant

Le profil de l'accédant non associé à une identité constitue une des données qui peut être transmise par la solution ENT aux services Tiers afin d'assurer l'authentification et le contrôle d'accès.

Il permet à un administrateur de donner des droits d'accès à une application en se basant sur ce profil et ainsi autoriser les accès (par exemple, autoriser les utilisateurs ayant le profil « Élève » à consulter une encyclopédie). Les informations de profils sont présentées par l'accédant dans le jeton de sécurité, ce qui permet de l'autoriser.

Chaque catégorie de profil de l'accédant **DOIT** être identifiée par un code unique sur le périmètre national.

Les profils de l'accédant sont par défaut peuplés automatiquement en fonction de la valeur d'un ou plusieurs attributs caractérisant les personnes. Ils peuvent être complétés de manière discrétionnaire.

Identifiant du profil de l'accédant (PROFIL_NATIONAL)	Description du périmètre
National_elv	Élève
National_tut	Responsable d'un élève (parent, tuteur légal)
National_ens	Enseignant non documentaliste
National_dir	Personnel de direction de l'établissement
National_evs	Personnel de vie scolaire travaillant dans l'établissement
National_eta	Personnel administratif, technique ou d'encadrement travaillant dans l'établissement
National_aca	Personnel non enseignant de rectorat, de DRAF, de DSDEN, de circonscription
National_doc	Documentaliste
National_col	Personnel de collectivité territoriale

Tableau 17 : Identifiants des profils de l'accédant

La valeur de l'identifiant du profil à fournir se détermine à partir de la classe d'objet puis de la fonction de la personne, comme le décrit le tableau ci-après :

Identifiant du profil	Classe d'objet 1er degré	Classe d'objet 2nd degré	Fonction
National_elv	ENTEleve	ENTEleve	(N/A)
National_tut	ENTPersRelEleve	ENTAuxPersRelEleve	(N/A)
National_ens	ENTEnseignant	ENTAuxEnseignant	ENS\$ENSEIGNEMENT
National_doc	(N/A)	ENTAuxEnseignant	DOC\$DOCUMENTATION
National_dir	(N/A)	ENTAuxNonEnsEtab	DIR\$DIRECTION
National_evs	(N/A)	ENTAuxNonEnsEtab	EDU\$EDUCATION
National_evs	(N/A)	ENTAuxNonEnsEtab	AED\$ASSISTANT D'EDUCATION

Identifiant du profil	Classe d'objet 1er degré	Classe d'objet 2nd degré	Fonction
National_evs	(N/A)	ENTAuxNonEnsEtab	SUR\$SURVEILLANCE
National_evs	(N/A)	ENTAuxNonEnsEtab	Autres cas
National_eta	(N/A)	ENTAuxNonEnsEtab	ADF\$PERSONNELS ADMINISTRATIFS
National_eta	(N/A)	ENTAuxNonEnsEtab	LAB\$PERSONNELS DE LABORATOIRE
National_eta	(N/A)	ENTAuxNonEnsEtab	ALB\$LABORATOIRE
National_eta	(N/A)	ENTAuxNonEnsEtab	MDS\$PERSONNELS MEDICO-SOCIAUX
National_eta	(N/A)	ENTAuxNonEnsEtab	OUV\$PERSONNELS OUVRIERS ET DE SERVICE
National_eta	(N/A)	ENTAuxNonEnsEtab	CTR\$CHEF DE TRAVAUX
National_eta	(N/A)	ENTAuxNonEnsEtab	ASE\$ASSISTANT ETRANGER
National_eta	(N/A)	ENTAuxNonEnsEtab	ORI\$ORIENTATION
National_eta	(N/A)	ENTAuxNonEnsEtab	CFC\$CONSEILLER EN FORMATION CONTINUE
National_eta	(N/A)	ENTAuxNonEnsEtab	Autres cas
National_aca	ENTNonEnsServAc	ENTAuxNonEnsServAc	(N/A)
National_col	ENTNonEnsCollLoc	ENTAuxNonEnsCollLoc	(N/A)

Tableau 18 : Détermination du profil de l'accédant à partir de la classe d'objet et de la fonction

Cette liste des fonctions associées à un profil de l'accédant demeure non exhaustive. Elle est liée aux fonctions transmises par le SI du ministère en charge de l'Éducation nationale.

Les porteurs de projet pourront ajouter d'autres fonctions, depuis la liste des fonctions fournie par la BCN, à certains profils recensés afin notamment de permettre l'interopérabilité avec les informations transmises par d'autres SI (par exemple SI du ministère en charge de l'enseignement agricole, SI de la collectivité territoriale).

5.8. Personnes en relation avec les élèves

5.8.1. Premier degré

Dans le premier degré, les personnes en relation avec l'élève sont décrites dans le champ ENTEleveAutoriteParentale qui contient les informations suivantes :

cle_jointure_person\$type_relation

Les différents éléments composant ce champ sont détaillés ci-après :

- cle_jointure_person : identifiant du responsable dans l'AAF pour l'Éducation nationale ;

- `type_relation` : les différentes valeurs possibles sont indiquées dans la nomenclature commune aux premier et second degrés `N_LIEN_ELEVE_RESPONSABLE`²⁰ (qui remplace l'ancienne nomenclature `N_LIEN_PARENTE_1D`).

5.8.2. Second degré

Dans le second degré et dans le but d'aligner les informations transmises aux solutions ENT avec celles saisies dans SIECLE (ex-SCONET), le champ `ENTElevePersRelEleve` contient les informations suivantes :

`cle_jointure_person$``type_relation$``resp_financier$``resp$``contact$``beneficiaire`

Les différents éléments composant ce champ sont détaillés ci-après :

- `cle_jointure_person` : identifiant du responsable dans l'AAF pour l'Éducation nationale ;
- `type_relation` : les différentes valeurs possibles sont indiquées dans la nomenclature commune aux premier et second degrés `N_LIEN_ELEVE_RESPONSABLE` (qui remplace l'ancienne nomenclature `N_LIEN_PARENTE`) ;
- `resp_financier` : s'appuie sur l'information « Paie les frais scolaires » dans SIECLE (responsable financier) ; 1 si la personne est responsable financier, 0 si la personne n'est pas responsable financier ;
- `resp` : les différentes valeurs possibles sont celles indiquées dans la nomenclature BCN commune aux premier et second degrés `N_NIVEAU_RESPONSABILITE` : 1 si la personne est « représentant légal », 2 si la personne est « personne en charge de l'élève », 3 si la personne est « personne à contacter » ;
- `contact` : s'appuie sur l'information de SIECLE concernant les représentants légaux et les personnes en charge de l'élève qui permet aux établissements d'indiquer si le responsable est à joindre en priorité ou non : 1 si la personne est à contacter en priorité, 0 sinon ;
- `beneficiaire` : s'appuie sur la nouvelle information « Perçoit les aides » dans SIECLE (les différentes valeurs possibles sont : 1 pour oui, 0 pour non).

Les combinaisons possibles pour les éléments `resp` et `contact` sont les suivantes :

Combinaisons possibles	Valeur <code>\$resp\$contact</code> dans <code>ENTElevePersRelEleve</code>
Représentant légal, à ne pas contacter en priorité	\$1\$0
Représentant légal, à contacter en priorité	\$1\$1
Personne en charge de l'élève, à ne pas contacter en priorité	\$2\$0
Personne en charge de l'élève, à contacter en priorité	\$2\$1
Personne à contacter	\$3\$0

Tableau 19 : Combinaisons possibles des éléments `resp` et `contact` dans le champ `ENTElevePersRelEleve`

Pour le niveau de responsabilité « personne à contacter » (niveau 3), les informations de la personne sont limitées à sa civilité, son lien avec l'élève, son nom de famille, son nom d'usage, son prénom et ses coordonnées téléphoniques.

²³ Les valeurs du niveau de formation et de la filière sont basées sur le MEF de rattachement (chaque MEF est associé à un MEF de rattachement et à un MEFSTAT).

5.9. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Nomenclatures	Chaque projet ENT DOIT être identifié par un code unique sur le périmètre national respectant la nomenclature définie dans l'annexe opérationnelle du SDET.	E	E
02	Nomenclatures	Chaque catégorie de profil de l'accédant DOIT être identifiée par un code unique sur le périmètre national respectant la nomenclature définie dans l'annexe opérationnelle du SDET.	E	E

Tableau 20 : Exigences et recommandations concernant les nomenclatures

6. Médiacentre

6.1. Introduction

Le Médiacentre de l'ENT est un espace qui regroupe les points d'accès vers les ressources pédagogiques éditoriales ou ressources numériques pour l'École (RNE) gratuites ou payantes, auxquelles l'utilisateur a droit dans le cadre de l'école ou l'établissement. Elles peuvent être externes ou intégrées à la solution ENT.

Le Médiacentre fait partie du service Accès aux ressources pédagogiques éditoriales de l'ENT (cf. Chapitre « Architecture de référence ENT » du document principal). Il est un espace à part entière de la solution ENT et représente pour l'utilisateur un espace distinct de son espace de stockage et de partage de fichiers.

6.2. Ressources du Médiacentre

Le Médiacentre présente à l'utilisateur l'ensemble de ses ressources pédagogiques éditoriales qui lui ont été affectées selon son identité, son profil, son appartenance à l'école ou l'établissement ou aux groupes et aux classes auxquels il est associé.

Cet ensemble est sous la responsabilité de l'école ou de l'établissement, en conséquence la typologie citée ci-après est une proposition qui peut être affinée en cohérence avec la politique de l'école ou l'établissement et les choix pédagogiques des équipes.

Dans le Médiacentre, l'utilisateur peut accéder notamment aux catégories définies pour les ressources accédées avec le GAR :

- ressources de référence, dictionnaires et encyclopédies ;
- manuels numériques ;
- ressources d'enseignement multimédias ;
- ressources de production pédagogique ;
- ressources d'entraînement et d'accompagnement scolaire ;
- ressources documentaires (Presse, etc.) ;
- ressources d'orientation.

Les ressources non décrites ou décrites selon des normes moins spécifiques pour l'enseignement scolaire pourront être rendues accessibles dans cet ensemble, dès lors que c'est un choix du projet ENT ou de l'équipe pédagogique de l'école ou de l'établissement (par exemple, accès au dictionnaire de l'académie française ou au Littré dans la catégorie « dictionnaires – encyclopédies »).

Les ressources du Médiacentre peuvent être des ressources externes à la solution ENT ou des ressources intégrées dans la solution ENT. Elles peuvent être des ressources accessibles via le GAR ou dans un autre cadre juridique ou réglementaire, identifiées par la pastille GAR accolée à la vignette de présentation.

Afin de simplifier la présentation des ressources dans le médiacentre, la distinction des ressources intégrées ou non ne devrait pas être affichée.

6.3. Fonctionnalités du Médiacentre

L'objectif principal du Médiacentre est la présentation organisée de l'ensemble des ressources pédagogiques éditoriales affectées à l'utilisateur dans le cadre de son (ses) école(s) ou son (ses) établissement(s). Cette présentation peut être organisée selon les catégories de ressources définies pour le GAR (cf. chapitre 5.2 « Ressources du Médiacentre »).

De plus, le Médiacentre peut trier les ressources selon d'autres critères : dates de dernière consultation, titres, matières ou domaines d'enseignement, favoris, etc.

Une fonctionnalité d'ajout de ressources à une liste de favoris devrait être proposée dans le Médiacentre afin de faciliter la navigation et améliorer l'expérience utilisateur.

Le Médiacentre devrait présenter un moteur de recherche sur les ressources, notamment pour les enseignants, afin de permettre aux utilisateurs de retrouver rapidement les ressources qu'ils souhaitent consulter. Une version de recherche avancée peut également être proposée en ajoutant des critères de recherche.

Le Médiacentre devrait permettre à l'utilisateur de filtrer ses ressources. Plusieurs axes de filtrage sont possibles : matière ou domaine d'enseignement, niveau éducatif pour les enseignants, type pédagogique de la ressource, typologie du document, catégorie de ressource, etc.

Les typologies utilisées pour permettre l'affichage des catégories de ressources pourront s'appuyer sur l'indexation ScoLOMFR²¹.

Le premier niveau d'affichage de chaque ressource doit être limité aux informations strictement nécessaires à l'utilisateur selon son profil. La présentation de chaque ressource dans le Médiacentre doit a minima contenir le titre, l'éditeur, la vignette, l'identifiant ark de la ressource. Le titre et la vignette permettent aux utilisateurs d'identifier et reconnaître les ressources. L'identifiant ark est nécessaire pour lever les ambiguïtés lors des demandes de support. Pour les ressources accessibles via le GAR, la vignette de la ressource doit être celle fournie par le GAR (qui comporte la pastille GAR).

²¹ <https://www.reseau-canope.fr/scolomfr/accueil.html>

6.4. Cas des utilisateurs multi-établissements

Par définition, le Médiacentre est attaché à une école ou un établissement (cf. chapitre 5.1 « Introduction ») et ce pour plusieurs raisons :

- C'est l'établissement qui est titulaire des abonnements. Le droit d'usage est attaché à l'établissement.
- L'usage de nombreuses ressources, en particulier des manuels, est conditionné au fait que l'enseignant et les élèves disposent des mêmes abonnements, et ces abonnements diffèrent d'un établissement à l'autre.
- Le médiacentre est le reflet de la politique documentaire de l'établissement, qui est une composante majeure de la mise en usage des ressources, notamment numériques.

Pour les utilisateurs multi-établissements, la solution ENT doit donc présenter un Médiacentre ou un onglet de Médiacentre par école / établissement.

6.5. Récapitulatif des exigences et recommandations

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Médiacentre	Afin de simplifier la présentation des ressources dans le médiacentre, la distinction des ressources intégrées ou non NE DEVRAIT PAS être affichée.	R	R
02	Médiacentre	La présentation des ressources pédagogiques éditoriales dans le Médiacentre PEUT être organisée selon les catégories de ressources définies par le GAR.	F	F
03	Médiacentre	Le Médiacentre DEVRAIT trier les ressources selon des critères autres que les catégories de ressources : dates de dernière consultation, titres, matières ou domaines d'enseignement, favoris, etc.	R	R
04	Médiacentre	Une fonctionnalité d'ajout de ressources à une liste de favoris DEVRAIT être proposée dans le Médiacentre.	R	R
05	Médiacentre	Le Médiacentre DEVRAIT présenter un moteur de recherche sur les ressources, notamment pour les enseignants.	R	R
06	Médiacentre	Le Médiacentre DEVRAIT permettre à l'utilisateur de filtrer ses ressources.	R	R
07	Médiacentre	La présentation de chaque ressource dans le Médiacentre DOIT a minima contenir le titre, l'éditeur, la vignette et l'identifiant ark de la ressource.	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
08	Médiacentre	Pour les ressources accessibles via le GAR, la vignette de la ressource DOIT être celle fournie par le GAR (qui comporte la pastille GAR).	E	E
09	Médiacentre	Pour les utilisateurs multi-établissements, la solution ENT DOIT donc présenter un Médiacentre ou un onglet de Médiacentre par école / établissement.	E	E

7. ENT et Gestionnaire d'accès aux ressources (GAR)

7.1. Introduction

L'accès unifié aux ressources numériques pour l'École est mis en œuvre grâce à un gestionnaire d'accès aux ressources (GAR) fondé sur un ensemble d'accords contractuels avec les fournisseurs de ressources impliqués et qui apporte les bénéfices suivants aux acteurs du projet ENT :

- une simplification des procédures techniques pour la connexion de la solution ENT aux distributeurs techniques de ressources, sur la base d'une adhésion volontaire du projet ENT au GAR. La solution ENT, au travers d'une seule adaptation pour le GAR, peut offrir aux utilisateurs l'accès à l'ensemble des ressources numériques pour l'École auxquelles ils ont droit dans son médiacentre ;
- une unification de l'affectation pour toutes les ressources, en proposant un service d'affectation aux établissements jusqu'au niveau individuel pour chaque ressource et chaque accédant (élève ou enseignant) autorisé, dans le respect du nombre de licences acquises ;
- une uniformisation de la présentation et de l'accès aux ressources regroupées dans le médiacentre ENT de l'utilisateur ;
- une simplification juridique, le GAR « tiers de confiance » permettant de filtrer d'une part des données des accédants transmises aux fournisseurs de ressources et d'autre part les données commerciales de ces derniers ;
- une protection des données à caractère personnel, le GAR assurant le respect du principe de proportionnalité.

Le présent chapitre présente donc succinctement les interactions entre l'ENT et le GAR. Pour plus de précisions, se reporter au référentiel technique, fonctionnel et de sécurité (RTFS) à destination des éditeurs/intégrateurs ENT et au [site GAR](https://gar.education.fr)²² dédié destiné à mettre à disposition les documentations relatives au GAR, au fur et à mesure de leur disponibilité.

²² Site du GAR (<https://gar.education.fr>)

7.2. Provisionnement des données du GAR

Pour fonctionner le GAR a besoin de données sur les structures et les utilisateurs.

Les projets ENT s'interfaçant avec le GAR sont donc sollicités pour fournir des extractions de leurs bases de données concernant :

- les établissements ;
- les élèves ;
- les personnels ;
- les groupes ;
- ainsi que les « responsables d'affectation » (utilisateurs chargés d'affecter les ressources aux élèves et enseignants).

7.3. ENT fournisseur d'identité

Quel que soit le mode d'authentification à l'ENT de l'utilisateur (auprès de l'ENT ou auprès d'un fournisseur d'identité externe), l'ENT joue un rôle de fournisseur d'identité vis-à-vis du GAR, que ce soit :

- pour l'élève ou l'enseignant qui accède à une ressource numérique depuis son ENT (et pour qui le GAR est « transparent » - l'utilisateur ne perçoit que les interfaces homme-machine (IHM) de l'ENT et de la ressource mais ne voit jamais le GAR lui-même) ;
- pour les responsables d'affectation qui accèdent au service d'affectation du GAR en mode de fédération d'identités depuis leur ENT.

7.4. Liste des ressources affectées

Un service fourni par le GAR permet à l'ENT d'interroger le GAR pour demander la liste des ressources affectées à un utilisateur.

En réponse, le GAR fournit à l'ENT la liste des ressources gérées par le GAR auxquelles l'utilisateur a droit, et pour chacune un ensemble « d'étiquettes ressource » décrivant de façon normalisée la ressource. L'ENT peut alors utiliser ces étiquettes ressources pour construire le **Médiacentre** de l'utilisateur (cf. chapitre 6 « Médiacentre »).

7.5. Accès à la ressource

Depuis le **Médiacentre**, l'utilisateur de l'ENT clique sur le lien d'accès à la ressource fourni dans les étiquettes ressource. L'ENT sollicite alors le GAR pour qu'il mette l'utilisateur en relation avec la ressource.

L'utilisateur peut également accéder à la ressource et l'utiliser dans le contexte de l'ENT en cliquant sur le lien depuis d'autres modules de l'ENT (par exemple le cahier de textes).

8. Ensemble annuaire

8.1. Documents de l'ensemble annuaire

L'ensemble annuaire est composé des documents listés ci-après.

Pour le premier degré :

- les spécifications de l'annuaire ENT pour le premier degré ;
- l'annexe 1 – dictionnaire des données ENT premier degré (format tableur) ;
- l'annexe 1bis – alimentation depuis le SI du MEN pour le premier degré ;
- la liste des évolutions des spécifications de l'annuaire premier degré.

Pour le second degré :

- le cahier des charges de l'annuaire ENT pour le second degré ;
- l'annexe 2 – caractérisation des personnes et des structures (format tableur) ;
- l'annexe 3 – schéma LDAP et nomenclatures (format tableur) ;
- l'annexe 4 – alimentation depuis le SI du MEN et depuis d'autres SI externes pour le second degré ;
- l'annexe 4 bis – alimentation depuis le SI du MEN et depuis d'autres SI externes pour le second degré (format tableur) ;
- la liste des évolutions du cahier des charges de l'annuaire ENT pour le second degré.

Pour les premier et second degrés :

- l'annexe 5 – exploitation et exploitabilité du service annuaire ENT.

8.2. Recommandations pour l'ensemble annuaire

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Annuaire ENT	<p>L'annuaire ENT pour le premier degré DOIT respecter les indications portées par les documents l'ensemble annuaire du SDET :</p> <ul style="list-style-type: none"> ▪ les spécifications de l'annuaire ENT pour le premier degré ; ▪ l'annexe 1 – dictionnaire des données ENT premier degré (format tableur) ; ▪ l'annexe 1bis – alimentation depuis le SI du MEN pour le premier degré ; ▪ l'annexe 5 – exploitation et exploitabilité du service annuaire ENT. 	E	N/A
02	Annuaire ENT	<p>L'annuaire ENT pour le second degré DOIT respecter les indications portées par les documents l'ensemble annuaire du SDET :</p> <ul style="list-style-type: none"> ▪ le cahier des charges de l'annuaire ENT pour le second degré ; ▪ l'annexe 2 – caractérisation des personnes et des structures ; ▪ l'annexe 3 – schéma LDAP et nomenclatures ; ▪ l'annexe 4 – alimentation depuis le SI du MEN et depuis d'autres SI externes pour le second degré ; ▪ l'annexe 4 bis – alimentation depuis le SI du MEN et depuis d'autres SI externes pour le second degré (format tableur) ; ▪ l'annexe 5 – exploitation et exploitabilité du service annuaire ENT. 	N/A	E

Tableau 21 : Exigences et recommandations concernant l'ensemble annuaire

9. Aspects juridiques

9.1. Préambule

Les aspects juridiques de l'annexe opérationnelle du SDET sont destinés à éclairer les porteurs de projets, les autorités académiques, les équipes d'accompagnement (personnels des DANE, des DSDEN, des circonscriptions, référents numériques) sur les éléments juridiques relatifs à la mise en œuvre et à l'exploitation d'un projet ENT.

Ce document est aussi l'occasion de rappeler les règles relatives à l'utilisation d'un ENT et s'adresse donc également, aux responsables de traitement (chefs d'établissement, IA-DASEN, le cas échéant collectivités territoriales) et aux utilisateurs.

Il est destiné à éclairer le lecteur dans sa compréhension des enjeux juridiques du cadre de confiance d'un projet ENT et d'un usage responsable.

Les présents chapitres ne se substituent ni au Code de l'éducation ni aux dispositions légales et réglementaires relatives aux ENT et plus généralement aux outils et services du numérique éducatif.

Ils ne se substituent pas non plus aux dispositions légales et réglementaires relatives à la protection des données à caractère personnel.

Enfin, ils peuvent compléter les contrats ou les marchés conclus pour le déploiement et la maintenance d'un projet ENT ainsi que les conditions d'utilisation d'un ENT.

9.2. Droit et ENT

L'ENT est l'une des composantes sur lesquelles s'appuie le service public du numérique éducatif. L'article L.131-2 alinéa 2 du Code de l'éducation prévoit que :

« Dans le cadre du service public de l'enseignement et afin de contribuer à ses missions, un service public du numérique éducatif et de l'enseignement à distance est organisé pour, notamment :

1° Mettre à disposition des écoles et des établissements scolaires une offre diversifiée de services numériques permettant de prolonger l'offre des enseignements qui y sont dispensés, d'enrichir les modalités d'enseignement et de faciliter la mise en œuvre d'une aide personnalisée à tous les élèves ;

2° Proposer aux enseignants une offre diversifiée de ressources pédagogiques, des contenus et des services contribuant à leur formation ainsi que des outils de suivi de leurs élèves et de communication avec les familles ;

3° Assurer l'instruction des enfants qui ne peuvent être scolarisés dans une école ou dans un établissement scolaire, notamment ceux à besoins éducatifs particuliers. Des supports numériques adaptés peuvent être fournis en fonction des besoins spécifiques de l'élève ;

4° Contribuer au développement de projets innovants et à des expérimentations pédagogiques favorisant les usages du numérique à l'école et la coopération.

Dans le cadre de ce service public, la détermination du choix des ressources utilisées tient compte de l'offre de logiciels libres et de documents au format ouvert, si elle existe. »

Parallèlement, le terme même « espace numérique de travail » est consacré dans différents textes de nature juridique.

9.2.1. Code de l'éducation

L'article D111- 5 du Code de l'éducation dispose que :

« Lors de sa première réunion, le conseil d'école ou le conseil d'administration examine les conditions d'organisation du dialogue avec les parents. Le conseil d'école ou le conseil d'administration peut prévoir toutes actions supplémentaires pour tenir compte des spécificités locales et des orientations du projet d'école ou d'établissement. Les conditions d'accueil des parents sont précisées, ainsi que les conditions dans lesquelles ils peuvent accéder aux espaces numériques de travail. Les parents d'élèves sont informés des décisions prises, notamment en ce qui concerne le nombre, la nature et la date des rencontres prévues. »

Cet article fixe les règles d'accès aux ENT pour les personnes responsables des élèves. L'ENT est ainsi un outil de dialogue et d'échange entre l'établissement ou l'école et les personnes responsables des élèves.

Le conseil d'école ou le conseil d'administration doit donc déterminer et informer les personnes responsables des élèves de leurs modalités d'accès aux espaces numériques de travail.

9.2.2. Code de la propriété intellectuelle

De plus, l'article L.122-5 3 e) du Code de la propriété intellectuelle dispose que :

*« Lorsque l'œuvre a été divulguée, l'auteur ne peut interdire (...) sous réserve que soient indiqués clairement le nom de l'auteur et la source (...) la représentation ou la reproduction d'extraits d'œuvres, sous réserve des œuvres conçues à des fins pédagogiques et des partitions de musique, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, y compris pour l'élaboration et la diffusion de sujets d'examens ou de concours organisés dans la prolongation des enseignements à l'exclusion de toute activité ludique ou récréative, dès lors que cette représentation ou cette reproduction est destinée, notamment au moyen d'un **espace numérique de travail**, à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés par l'acte d'enseignement, de formation ou l'activité de recherche nécessitant cette représentation ou cette reproduction, qu'elle ne fait l'objet d'aucune publication ou diffusion à un tiers au public ainsi constitué, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire sans préjudice de la cession du droit de reproduction par reprographie mentionnée à l'article L.122-10 ».*

9.2.3. Loi relative à l'Informatique, aux fichiers et aux libertés modifiée & RGPD

Les espaces numériques de travail (ENT) impliquent des traitements de données à caractère personnel qui doivent être mis en œuvre conformément au RGPD et à la loi relative à l'Informatique, aux fichiers et libertés modifiée.

Dans ce cadre, chaque responsable de traitement est tenu de respecter les principes relatifs au traitement de données personnelles (base juridique, loyauté et transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité...) conformément aux articles 5 du RGPD et 4 de la loi relative à l'Informatique, aux fichiers et aux libertés modifiée. L'article 4 de la loi prévoit que :

« Les données à caractère personnel doivent être :

- a) *traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;*
- b) *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;*
- c) *adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;*
- d) *exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;*
- e) *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ;*
- f) *traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées. »*

Dans ce cadre, chaque responsable de traitement doit veiller au respect des droits des personnes concernées (articles 12 à 23 du RGPD), des principes de protection par défaut et dès la conception des données (article 25 du RGPD), ainsi que des obligations de sécurité issues notamment de l'article 32 du RGPD.

Chaque responsable de traitement se doit encore de procéder aux conventionnements requis, c'est-à-dire à la formalisation de contrat de responsabilité de traitement conjointe avec les autres responsables de traitement (article 26 du RGPD) et, à une parfaite vigilance sur l'intégration d'une clause de sous-traitance conforme aux exigences de l'article 28 du RGPD dans le marché signé avec l'éditeur de la solution ENT.

En outre, chaque responsable de traitement veille à procéder à l'inscription du traitement de données personnelles relatif aux ENT au sein de son registre des traitements conformément à l'article 30 du RGPD.

9.2.4. Circulaires

Un ensemble de circulaires vient préciser les modalités d'usage des ENT dans le cadre des écoles et des établissements.

Déjà en 2010, la circulaire de rentrée n° 2010-38 du 16 mars 2010 imposait le développement du numérique à l'école et visait notamment en priorité la généralisation des ENT et du cahier de textes numérique.

La circulaire d'orientation et d'instructions pour la préparation de la rentrée 2012 n° 2012-056 du 27 mars 2012 visait la généralisation des ENT afin d'offrir un accès sécurisé et simplifié à un nombre croissant de services et des ressources pédagogiques et éducatives aux élèves.

En 2013, la circulaire d'orientation et de préparation de la rentrée n° 2013-060 du 10 avril 2013 confirmait la poursuite de la généralisation des ENT dans les académies, en étroite collaboration avec les collectivités territoriales afin d'assurer notamment une implication plus forte des parents dans le cadre de l'enseignement.

La circulaire de rentrée 2014 n° 2014-068 du 20 mai 2014 introduisait l'intérêt de l'ENT en classe et hors de la classe, afin d'offrir à la communauté éducative un ensemble intégré de services numériques, choisi, organisé par l'établissement scolaire.

En 2015, la circulaire de rentrée n° 2015-085 du 3 juin 2015 rappelait à nouveau le principe de généralisation des ENT.

La circulaire de rentrée n° 2016-058 du 13 avril 2016 précise que dans le cadre du Plan numérique pour favoriser la généralisation des usages pédagogiques du numérique : *« L'École a la responsabilité de développer un cadre de confiance, protecteur des données des élèves. En garantissant la sécurité et la protection des données personnelles, sociales et scolaires, les espaces numériques de travail (ENT) offrent d'ores et déjà à l'ensemble de la communauté éducative de l'école ou de l'établissement un accès unifié à un bouquet de ressources et de services numériques pour les usages pédagogiques et éducatifs »*. Ladite circulaire précise que *« dans le cadre d'un partenariat étroit et renforcé avec les collectivités territoriales, la poursuite de la généralisation des ENT dans les premier et second degrés s'accompagnera, dans le respect du droit des usagers, d'une plus grande ouverture à de nouveaux services et à des usages nomades dans et hors de l'École, sur tous types de support, mobiles ou non »*.

En 2017, la circulaire de rentrée n° 2017-045 du 9-3-2017 inscrit les ENT dans le cadre de la transformation numérique de l'École qui repose sur le développement d'un **environnement de confiance, protecteur des données des élèves**. Elle précise : *« Dans cette perspective, les espaces numériques de travail (ENT), en lien avec le gestionnaire d'accès aux ressources (GAR), permettent un accès simplifié aux ressources numériques des établissements. Les ENT, qui mettent à la disposition de l'ensemble de la communauté éducative des services de communication et de collaboration, répondent aux nouveaux usages en mobilité et facilitent les échanges entre les degrés et entre les établissements »*.

9.2.5. Référentiels

Enfin l'ENT est également visé dans différents référentiels qu'il s'agisse :

- du Cadre de référence pour l'accès aux ressources pédagogiques via un équipement mobile (CARMO) qui sert de référence dans les projets mobilité pour l'Éducation, et dans les exigences formulées dans les contrats passés avec les différents prestataires ; la classification de quatre catégories de services fonctionnels sur cinq reprend celle du SDET pour prendre en compte les accès aux ENT depuis les équipements individuels mobiles ;
- du Cadre de référence des services d'infrastructures numériques d'établissements scolaires et d'écoles (CARINE) qui prévoit notamment l'intégration d'un ENT dans l'écosystème existant de l'établissement ;
- du Référentiel sur l'usage du Wi-Fi en établissement et école qui prévoit le cadre juridique des usages associés du réseau Wi-Fi de l'établissement et notamment l'accès à l'espace numérique de travail (ENT) ;
- du Schéma directeur des infrastructures du MENESR 2010-2015 (SDI) qui prévoit que le déploiement à l'échelle académique des projets ENT, en partenariat avec les collectivités, conduit à une croissance des besoins spécifiques d'évolution du système d'information académique imposant de préserver au niveau académique les capacités et l'autonomie nécessaires ;
- du Référentiel technique, fonctionnel et de sécurité (RTFS²³) du GAR qui fournit l'ensemble des informations techniques, fonctionnelles et de sécurité permettant aux éditeurs et aux intégrateurs ENT de s'interfacer avec le Gestionnaire d'accès aux ressources numériques (GAR).

9.2.6. Espace de droit

D'une manière plus générale l'ENT est un **espace de droit**.

Il s'agit d'abord d'un outil au service de la pédagogie. À ce titre, il se voit donc appliquer les dispositions du Code de l'éducation pour les dispositions qui lui sont pertinentes.

9.2.6.1.1. Espace intégré de services et contenus numériques

L'ENT est par nature un ensemble intégré de services et contenus numériques et se voit appliquer, de fait, d'autres réglementations telles que le droit de l'internet ou des communications électroniques.

L'ENT permet d'effectuer des démarches ou des formalités administratives, des échanges et collaborations entre écoles et établissements d'un même ENT ou d'ENT différents, ainsi que l'accès à des services Tiers en dehors du périmètre de responsabilité de l'ENT.

²³ Téléchargeable sur le site du GAR (<https://gar.education.fr>)

9.2.7. Espace de travail

L'ENT est aussi un espace de travail pour l'ensemble de la communauté éducative tel que mentionné dans la définition même des ENT qui s'appuie sur l'article L.111-3 du Code de l'éducation²⁴.

À ce titre, pour les enseignants, l'ENT se verra appliquer les règles relatives aux droits et obligations des agents de la fonction publique et les règles d'organisation professionnelle qui y sont attachées.

Concernant les élèves, la notion de travail renvoie au caractère éducatif et pédagogique de cet espace. À ce titre, les usages de l'ENT devront être conformes à sa destination et remplir les objectifs d'enseignement et d'échanges entre les membres de la communauté éducative.

L'ENT est également un espace d'échanges de documentations et d'informations administratives relatives à la vie scolaire, aux enseignements et au fonctionnement de l'école ou de l'établissement.

Les ENT ont une fonction dédiée. Il ne s'agit pas d'espaces numériques génériques tels que les médias ou les réseaux sociaux.

En tout état de cause, en tant qu'espace de travail, l'ENT se verra appliquer l'ensemble des règles relatives à la régulation des contenus et au droit de la propriété intellectuelle.

9.2.8. À retenir



L'ENT est un espace de droit. L'ensemble des parties prenantes au projet ENT, porteurs de projet, autorités académiques, équipes d'accompagnement et utilisateurs, doit respecter les dispositions législatives et réglementaires (droit des marchés publics et des contrats, droit de la responsabilité, droit de l'internet, droit de la propriété intellectuelle, droit de la protection des données personnelles...).

9.3. Contrats et ENT

Comme il a été indiqué précédemment, l'ENT est un espace qui s'inscrit dans un cadre législatif et réglementaire mais aussi contractuel.

Ce cadre contractuel correspond à différentes situations : la mise en œuvre, l'exploitation et la maintenance d'une solution l'ENT, l'usage de l'ENT, l'utilisation des contenus de l'ENT, l'interconnexion d'une solution ENT avec d'autres environnements dont les espaces de travail collaboratif entre ENT.

Par conséquent différents niveaux de relations contractuelles sont envisageables.

²⁴ Article L.111-3 du Code de l'éducation : « 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 »

9.3.1. Premier niveau : portage du projet ENT via une convention de partenariat

Le projet peut impliquer les collectivités territoriales concernées, les autorités académiques, les écoles, les établissements. La maîtrise d'ouvrage sera représentée généralement par les collectivités territoriales en partenariat avec les académies (cf. Chapitre « Objectifs et positionnement du SDET » du document principal).

Il est recommandé de conclure une convention cadre²⁵ de partenariat entre porteurs de projet que sont les collectivités territoriales ou groupements de collectivités et les académies notamment. Le ou les prestataires chargés de la fourniture et de la mise en œuvre des solutions ENT sont sélectionnés par les parties au titre d'accords distincts et ne constituent pas des parties à la convention cadre.

La convention devrait avoir pour objet de définir les rôles et engagements des parties, relatifs à la promotion, l'accompagnement, la formation et l'assistance pour la mise en œuvre de l'ENT, la fourniture, au bénéfice des responsables de traitements, des données à caractère personnel nécessaires ainsi qu'un cadre de gouvernance et de pilotage.

Afin que les collectivités territoriales le souhaitant puissent rejoindre la convention cadre de partenariat, un mécanisme d'adhésion gagnerait à être prévu dans la convention cadre.

En tout état de cause, la convention devrait être adaptée pour tenir compte de la réalité opérationnelle de chaque projet. Elle peut concerner par exemple d'autres structures que les établissements scolaires du premier et/ou du second degré.

Dans le cas particulier de l'extraction de données des annuaires ENT pour alimenter en données à caractère personnel les solutions de gestion des équipements fixes et mobiles et de gestion de classe conformes aux cadres de référence CARINE et CARMO, une convention de partenariat entre l'État et les collectivités territoriales concernées s'impose. Cette convention définit les modalités et conditions d'exploitation des données et en rappelle notamment les finalités. Cette extraction peut être opérée uniquement si le traitement est inscrit dans le registre du responsable de traitement et permet une extraction pour une telle finalité.

9.3.2. Deuxième niveau : sécurisation des traitements de données personnelles via une convention de responsabilité de traitement conjointe adossée à la convention de partenariat

Comme évoqué *supra*, un projet ENT peut être porté par plusieurs parties prenantes, soit notamment outre les autorités académiques et les établissements publics locaux d'enseignement, une ou plusieurs collectivités territoriales. Or, dès lors que ces différentes entités participent aux décisions stratégiques du projet et sont ainsi impliquées dans la détermination des finalités et des moyens des traitements de données à caractère personnel associés, elles recouvrent la qualité de responsable de traitement au sens de l'article 4 du RGPD.

²⁵ Un contrat cadre est un accord par lequel les parties conviennent des caractéristiques générales de leurs relations contractuelles futures, selon l'article 1111 du code civil.

Par suite et conformément aux dispositions de l'article 26 du RGPD, une convention de responsabilité de traitement conjointe doit impérativement être formalisée entre ces différentes entités.

La difficulté procède toutefois de ce qu'il n'existe pas nécessairement de corrélation entre les parties à la convention de partenariat et celles tenues à l'obligation précitée de contractualisation sur les enjeux de protection des données à caractère personnel.

En effet, si les établissements publics locaux d'enseignement assument une part de responsabilité de traitement, dès lors qu'il leur appartient, notamment, de déterminer les modules de l'ENT dont ils entendent se doter, ils ne sont pas systématiquement signataires des conventions de partenariat.

C'est pourquoi et par souci de lisibilité, il demeure, à ce jour, plus aisé de formaliser une convention de responsabilité de traitement conjointe se référant à la convention de partenariat mais lui étant pour autant distincte.

Si une grande latitude est consentie aux parties dans la formalisation de ce type de convention, laquelle se doit de clarifier les responsabilités assumées par chacune des parties à l'égard des traitements en cause, **des modèles types de convention sont néanmoins mis à leur disposition sur Éduscol au sein d'un kit dédié précisément au respect des exigences contractuelles issues de la réglementation Informatique et Libertés.**

9.3.3. Troisième niveau : réalisation et acquisition d'une solution ENT

Aux fins de réalisation de l'ENT, un cahier des charges fonctionnel et technique est rédigé en vue de la sélection d'un prestataire pour la mise en œuvre et le déploiement de la solution ENT.

L'acquisition de la solution ENT suit les règles de la commande publique. La sélection du prestataire fournisseur de la solution ENT, la réalisation de la solution et sa mise en œuvre se conforment aux dispositions légales relatives aux marchés publics.

Les éditeurs, intégrateurs, exploitants ENT assurent la maîtrise d'œuvre, définie dans la le marché public de la maîtrise d'ouvrage ou à défaut, dans un contrat de prestations.

Quels que soient la nature et le choix du type de solution ENT, des clauses standards doivent être prévues dans chaque contrat technique : recette, maintenance, propriété, garanties, sécurité, responsabilité, qualité de service, réversibilité et portabilité des données, etc.

Une clause adaptée doit prévoir et faciliter la réversibilité des projets ENT et ainsi préciser les exigences et recommandations en cas de renouvellement/changement du marché et/ou du prestataire au cours du marché. Il doit être apporté un soin particulier, par le porteur de projet dans son cahier des charges, à la rédaction de cette clause afin de permettre la continuité des projets ENT.

Une clause de sous-traitance conforme aux exigences de l'article 28 du RGPD doit encore impérativement être intégrée à ce type de contrat. Il est à cet effet également recommandé, de solliciter, dans les documents de la candidature liée à la consultation en cause, une politique de protection des données à caractère personnel pour être en mesure de vérifier les garanties de sécurité desdits candidats. La portabilité de données personnelles des utilisateurs entre ENT doit permettre de faciliter la reprise de données en cas de réversibilité et la transition entre solutions ENT différentes.

Eu égard aux éléments que peut intégrer la solution ENT, il est important que l'éditeur de l'ENT garantisse le respect des droits des tiers via l'encadrement contractuel relatif à l'utilisation de ces éléments (cf. chapitre 9.12 Droit des tiers).

Le logiciel ou le contenu, qu'il soit libre ou propriétaire, est une œuvre de l'esprit protégée par les règles du droit d'auteur, dès lors qu'il présente un caractère original²⁶. Le logiciel libre est soumis à des conditions d'utilisation des droits définis par les auteurs ou propriétaires des droits. Généralement ces conditions sont organisées dans un contrat de licence.

Que le logiciel ou contenu soit libre ou propriétaire, il convient d'apporter une attention particulière aux licences correspondantes afin d'éviter tout acte de contrefaçon.

9.3.3.1. Hébergement

L'hébergement d'une solution ENT peut se faire par infogérance :

- auprès d'une société de services en ingénierie informatique (SSII) ;
- ou auprès d'un service informatique de la collectivité territoriale ou de l'académie ;
- ou auprès d'une société proposant une solution ENT en mode SaaS²⁷.

Dans l'hypothèse de l'infogérance, plusieurs acteurs seront amenés à intervenir. Les relations avec chaque professionnel devront être contractuellement encadrées et préciser les règles de sécurité qui leur sont applicables dans le cadre de l'hébergement de l'ENT et des prestations associées à cet hébergement. Ce document contractuel devra contenir une annexe protection des données qui répond aux dispositions du RGPD et de la loi relative à l'Informatique, aux fichiers et libertés modifiée. Cette annexe devra apporter des garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et de la loi relative à l'Informatique, aux fichiers et libertés modifiée et garantisse la protection des droits de la personne concernée.

L'hébergeur s'engage à héberger les données dans un pays membre de l'Union européenne, ou avec l'autorisation expresse du responsable de traitement, dans des pays qui assurent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. En cas de transferts de données personnelles vers des pays hors Union européenne, le prestataire devra justifier de l'adoption d'un ou plusieurs outils reconnus par le RGPD pour permettre aux acteurs d'apporter un niveau de protection suffisant : les règles internes d'entreprise (ou BCR), les clauses contractuelles types (CCT) ...

9.3.3.2. ENT et services Tiers

Les services natifs et les applications métier²⁸ intégrées à l'ENT entrent dans le cadre de confiance tel que créé par le présent schéma directeur.

L'accès aux services Tiers est historiquement consacré comme une finalité du traitement de données à caractère personnel mis en œuvre dans le cadre d'un ENT. Elle devra être visée dans le registre des traitements du responsable de traitement et être portée à la connaissance des personnes concernées²⁹.

²⁶ Article L.112-2° du Code de la propriété intellectuelle

²⁷ SaaS : acronyme pour Software as a Service. Le mode SaaS est un mode d'utilisation d'une solution logicielle qui se fait en utilisant l'application à distance qui est hébergée par l'éditeur.

²⁸ Applications métier intégrées : ensemble applicatif inclus dans un projet ENT venant compléter la solution éditeur. Il présente un cycle de vie et un niveau d'intégration avec la solution ENT complètement défini et maîtrisé par le projet ENT. Cet ensemble applicatif rentre ainsi de fait dans le cadre de confiance de l'ENT.

²⁹ Arrêté du 30 novembre 2006 portant création, au sein du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, d'un traitement de données à caractère personnel relatif aux espaces numériques de travail (ENT) modifié par l'arrêté du 13 octobre 2017, article 1.

Sont considérés comme services Tiers, les services externes à la solution ENT mise en œuvre au travers d'un projet ENT. Ces services peuvent nécessiter un cadre juridique particulier lorsque des données à caractère personnel sont transmises à des tiers ou stockées en dehors du cadre de confiance (cf. chapitre « Cadre de confiance » du document principal pour plus de détails).

Le responsable de traitement de l'ENT ne doit pas donner accès aux utilisateurs vers les services Tiers si ces derniers ne respectent pas le SDET. Le responsable de traitement doit procéder aux vérifications nécessaires. Les destinataires devront figurer dans le registre des traitements du responsable de traitement ainsi que dans l'information portée à la connaissance des personnes concernées conformément au RGPD.

L'interfaçage entre l'ENT et des services Tiers implique dès lors la signature d'une convention de service avec les fournisseurs de services Tiers (comme précisé dans le chapitre 9.3.3.2.1 Convention de service) ou une adhésion au GAR.

9.3.3.2.1. Convention de service

Concernant l'interopérabilité de la solution ENT avec des services Tiers, une convention de service doit être élaborée entre les porteurs de projets et les fournisseurs de services Tiers concernés ainsi qu'avec les responsables de traitement dans le cas de transmission de données à caractère personnel. Celle-ci doit permettre de préciser leurs rôles respectifs, leurs engagements et les modalités de traitement des données à caractère personnel des utilisateurs soient précisément définis.

La convention de service³⁰ doit contenir un certain nombre de clauses et doit notamment définir :

- les engagements des acteurs ;
- l'organisation, les conditions (qualité de service par exemple) et modalités d'inscription/retrait au service Tiers ;
- les transferts de données ;
- la possibilité de sous-traitance ;
- la possibilité de réversibilité.

Lorsque la convention de service identifie un sous-traitant au sens du RGPD, elle doit contenir une annexe protection des données reprenant au minimum l'ensemble des prescriptions de l'article 28 du RGPD.

Les services Tiers dont les fournisseurs n'ont pas adhéré aux accords contractuels du GAR devront s'inscrire dans les différents cas de figure du tableau présenté au chapitre 2.6 « Exigences et recommandations pour l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités » afin de s'inscrire dans le cadre de confiance offert par le SDET.

9.3.3.2.2. Le Gestionnaire d'accès aux ressources (GAR)

La solution ENT pourra également s'interfacer avec d'autres services Tiers via le GAR permettant de garantir le cadre de confiance. La CNIL l'encourage et note que le dispositif s'inscrit dans l'esprit du RGPD³¹. En pratique le contrat d'adhésion au GAR des services tiers comprend également une charte éthique.

³⁰ cf. chapitre 2.6.3 « Conventions de service »

³¹ Délibération n°2017-253 du 21 septembre 2017 portant avis sur un projet d'arrêté relatif à la mise en œuvre par le ministère de l'éducation nationale d'un traitement de données à caractère personnel dénommé gestionnaire d'accès aux ressources (AV n°17000891)

Ainsi, dans un premier temps, les fournisseurs de ressources doivent s'engager en signant un contrat d'adhésion et respecter un référentiel technique et fonctionnel. Dans un second temps, la mise en œuvre du traitement de données à caractère personnel permet aux utilisateurs et partenaires de bénéficier des services du GAR et de transmettre aux fournisseurs de ressources adhérents uniquement les données identifiées en amont comme nécessaires³².

La liste des acteurs ENT (éditeurs, intégrateurs ENT, projets ENT) et des fournisseurs de ressources adhérents au GAR est publiée sur le [site du GAR](#)³³.

9.3.4. Quatrième niveau : contrats avec les utilisateurs

Préalablement à toute utilisation, les utilisateurs de l'ENT devront prendre connaissance et accepter la charte d'usage des services numériques rappelant les droits et les obligations des parties. Pour cela, il est renvoyé au chapitre relatif aux conditions d'utilisation.

9.3.5. À retenir



La mise en œuvre d'un projet ENT impose que soit rédigé un ensemble contractuel destiné à délimiter le périmètre d'intervention des différents acteurs impliqués, leurs obligations, leurs responsabilités et leurs engagements.

9.4. Accès et conditions d'utilisation

Les conditions d'accès, d'utilisation et de fonctionnement de l'ENT sont généralement fixées dans un document de référence dénommé « charte d'usage des services numériques », au sein de laquelle figureront des dispositions se rapportant aux ENT.

Ces règles sont de nature contractuelle. L'utilisateur doit les accepter lors de sa première connexion à l'ENT.

L'utilisateur de l'ENT doit respecter les règles qui lui sont ainsi fixées. À défaut il pourra être sanctionné de différentes manières (restriction d'usage, suppression de compte, sanction disciplinaire...).

La terminologie et la forme de la charte d'usage des services numériques importent peu, l'essentiel étant que ses conditions :

- soient claires dans leur rédaction ;

³² Arrêté du 18 décembre 2017 relatif à la mise en œuvre par le ministère de l'éducation nationale d'un traitement de données à caractère personnel dénommé « gestionnaire d'accès aux ressources » (GAR) (<https://www.legifrance.gouv.fr/eli/arrete/2017/12/18/MENN1729109A/jo/texte/fr>)

³³ Site du GAR (<https://gar.education.fr>)

- soient acceptées formellement par les utilisateurs lors de leur première connexion pour leur être opposables.

La charte d'usage des services numériques vient ainsi compléter d'autres documents tels que le règlement intérieur des écoles et des établissements.

La charte d'usage des services numériques doit énoncer les différentes règles de droit s'appliquant à l'utilisation de l'ENT. Elle comprend de manière non exhaustive, le respect de la vie privée, du droit à l'image, de la propriété intellectuelle, de la protection des données, la responsabilité du directeur de publication dans les espaces partagés. La charte d'usage des services numériques doit également inciter les usagers à respecter les conditions de sécurité entourant l'ENT et à ne commettre aucun acte illicite ou portant atteinte aux droits des tiers.

Cette charte d'usage des services numériques doit également rappeler les principes de l'Éducation nationale et notamment le principe de neutralité religieuse, politique et commerciale.

9.4.1. Droits des utilisateurs

La charte d'usage des services numériques rappelle les droits des utilisateurs et notamment :

- les conditions dans lesquelles les utilisateurs ont le droit d'accéder à l'ENT en précisant les services de base et les services complémentaires auxquels les utilisateurs accèdent suivant leur catégorie ;
- la possibilité de stocker du contenu dans l'ENT ;
- tous les droits informatiques et libertés et notamment le droit d'accès à ses données à caractère personnel
- le droit au respect de la vie privée résiduelle ;
- les conditions d'accès et d'échanges aux espaces de contributions personnelles, aux espaces, de stockage d'informations individuelles et aux espaces de commentaires et de publication.

9.4.2. Obligations des utilisateurs

La charte d'usage des services numériques rappelle également les obligations des utilisateurs parmi lesquelles :

- le respect du principe de neutralité religieuse, politique et commerciale ;
- le respect des droits des tiers ;
- l'interdiction de diffuser et d'accéder à des contenus illicites ;
- le respect des finalités de l'ENT ;
- le respect de l'intégrité technique des systèmes d'information.

9.4.3. Identification / authentification

La charte d'usage des services numériques souligne le caractère éminemment personnel du couple identifiant / mot de passe permettant d'accéder aux services de l'ENT. Ce rappel permet d'introduire le principe suivant lequel toute utilisation du mot de passe est présumée effectuée au nom de l'utilisateur, de sorte que l'utilisateur demeurera seul responsable de l'utilisation de l'ENT qui sera faite sous son identifiant.

9.4.4. Responsabilité

Outre les éléments de responsabilité généraux, la charte d'usage des services numériques à destination des utilisateurs précise que l'utilisateur est responsable de l'utilisation de son espace individuel et des contributions qu'il publie et des informations qu'il échange.

9.4.5. Obligation de protection des données personnelles

S'agissant de l'ENT, la charte d'usage des services numériques précise que le ou les responsable(s) du traitement met(tent) en œuvre un traitement de données à caractère personnel ainsi que les caractéristiques dudit traitement (finalités, base légale, catégorie de données collectées, conditions de collecte, destinataires, durée de conservation).

La charte d'usage des services numériques informe également l'utilisateur des droits dont il dispose concernant la protection de ses données à caractère personnel et précise les modalités d'exercice de ses droits.

9.4.6. À retenir



La mise en œuvre d'un projet ENT impose :

- la rédaction de conditions d'utilisation contenant les clauses relatives aux droits des usagers, à leurs obligations, aux responsabilités attachées à l'utilisation de l'ENT ainsi qu'aux sanctions éventuelles ;
- un processus d'acceptation de ces conditions d'utilisation en vue de s'assurer de leur opposabilité.

9.5. Protection des données à caractère personnel

9.5.1. Principes fondamentaux applicables au traitement des données à caractère personnel

Un ENT donne lieu à un traitement de données à caractère personnel. De fait, l'ENT s'inscrit nécessairement dans le cadre du respect du RGPD, entré en application le 25 mai 2018 et de la loi relative à l'Informatique, aux fichiers et libertés modifiée.

L'ENT peut être mis en œuvre dans les écoles, les établissements publics locaux d'enseignement (EPL), les établissements d'enseignements privés sous contrat, les centres de formation d'apprentis de l'Éducation nationale. Il peut être également mis en œuvre dans tout autre établissement pour lequel le responsable de traitement a procédé notamment à l'inscription du traitement de données personnelles relatif aux ENT au sein de son registre des traitements conformément à l'article 30 du RGPD).

Le registre indique au minimum :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 du RGPD.

Il est recommandé de contacter son délégué à la protection des données (DPD) académique si une aide est nécessaire afin de renseigner les fiches registres.

L'ensemble des traitements des données à caractère personnel mis en œuvre dans le cadre d'un ENT doit être effectué conformément aux obligations issues du RGPD. En particulier, le déploiement d'un ENT doit s'inscrire dans une démarche de protection dès la conception³⁴ et de protection par défaut³⁵ des données à caractère personnel.

³⁴ La notion de protection dès la conception consiste en l'application des principes relatifs à la protection des données dès la création d'un traitement et tout au long de son cycle de vie.

³⁵ La protection des données par défaut consiste à faire en sorte que, par défaut, les fonctionnalités des applications contenant des données personnelles garantissent un très haut niveau de protection des données en s'assurant sans autre action notamment que seules les données nécessaires soient traitées.

Pour répondre à l'obligation de protection des données dès la conception, le ou les responsable(s) de traitement applique(nt), tant lors de la détermination des moyens mis en œuvre pour le traitement que pendant le traitement lui-même, des mesures techniques et organisationnelles appropriées pour l'activité de traitement menée et ses objectifs, notamment la minimisation et la pseudonymisation, de manière à ce que le traitement soit conforme au RGPD et à la loi relative à l'Informatique, aux fichiers et libertés modifiée et que le traitement assure la protection des droits de la personne concernée, en tenant compte notamment :

- de l'état des connaissances (état de l'art) ;
- des coûts de mise en œuvre ;
- des finalités du traitement ;
- des risques concernant l'atteinte aux droits et libertés des personnes physiques.

Pour répondre à l'obligation de protection des données par défaut, le responsable de traitement doit garantir que les exigences de protection des données soient prises en compte de manière opérationnelle sans nécessiter une intervention volontaire de la personne concernée.

Cette implémentation correspond à la mise en œuvre de mesures techniques ou organisationnelles.

De plus, les traitements doivent respecter un certain nombre de principes directeurs applicables à tous les traitements parmi lesquels le principe de minimisation.

La minimisation impose d'éviter de traiter des données à caractère personnel sauf si pour atteindre l'objectif recherché, il est impossible ou très difficile de faire autrement (article 5, article 25 § 1, article 47 § 2 d et article 89 § 1 du RGPD).

L'ensemble des traitements de données à caractère personnel mis en œuvre par un ENT doit être inscrit dans le registre des traitements par le responsable du traitement.

Il est recommandé de contacter son délégué à la protection des données (DPD) académique si une aide est nécessaire afin de renseigner les fiches registres.

Le responsable de traitement doit identifier la base juridique de chacun des traitements mis en œuvre dans le cadre de l'ENT et déterminer s'il s'agit d'une mission d'intérêt public ou relevant de l'exercice d'une autorité publique ou encore d'une autre base juridique visée par l'article 6 du RGPD.

La base juridique d'un traitement de données à caractère personnel doit être définie avant la collecte des données.

Les finalités poursuivies par le traitement des données à caractère personnel doivent être déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (article 5 du RGPD et article 4 de la loi relative à l'Informatique, aux fichiers et libertés modifiée). Le responsable de traitement doit en ce sens limiter la collecte des données à ce qui est nécessaire à la finalité poursuivie. Par ailleurs, cette finalité doit être portée à la connaissance des personnes concernées de manière accessible, facile à comprendre. Elle doit être formulée en des termes clairs et simples.

Les finalités des traitements devraient être celles visées dans l'ancien arrêté du 30 novembre 2006 modifié en 2017 qui demeure une référence utile à ce jour :

- saisir et mettre à la disposition des élèves ou des personnes responsables des élèves, des enseignants, des personnels administratifs, des équipes d'accompagnement et plus généralement, de tous les membres de la communauté éducative de l'enseignement scolaire, en fonction des habilitations de chaque usager, des contenus éducatifs et pédagogiques, des informations administratives, relatives à la vie scolaire, aux enseignements et au fonctionnement de l'école ou de l'établissement ainsi que de la documentation en ligne ;
- permettre des échanges et des collaborations entre écoles et établissements d'un même ENT ainsi qu'avec des écoles et des établissements utilisant des ENT différents ;
- permettre, dans le respect des dispositions du RGPD, un accès à des services Tiers ;
- permettre une finalité statistique en vue de procéder à la mesure des accès aux différents services proposés.

Les données traitées pour réaliser ces finalités doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de ces finalités pour lesquelles elles sont traitées, conformément au principe de minimisation des données.

Selon ce principe, les catégories de données traitées devraient a minima être celles visées dans l'ancien arrêté du 30 novembre 2006 modifié en 2017 lequel n'a plus de valeur prescriptive mais demeure un document de référence utile. Elles sont soit issues des systèmes d'information mis en œuvre par les ministères dont les écoles et les établissements scolaires relèvent ou des systèmes d'information mis en œuvre par les collectivités territoriales, soit fournies par les usagers des ENT. Elles pourront le cas échéant être complétées en fonction de la solution mise en œuvre.

Dans le cadre d'un ENT, il est nécessaire d'identifier les personnes qui sont destinataires de données³⁶.

À cet égard, les destinataires devraient être ceux visés dans l'arrêté du 30 novembre 2006 modifié en 2017.

En tout état de cause, ces destinataires doivent être limités aux seules personnes dont l'accès aux données est justifié pour l'exécution d'une mission particulière ou d'une prestation selon le principe du moindre privilège³⁷.

Le traitement effectué devra répondre à l'exigence de transparence et de loyauté selon laquelle le responsable de traitement doit informer et communiquer les modalités d'exercice des droits des personnes aux personnes concernées.

Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible, facile à comprendre, formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels.

Le jeune public méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en termes clairs et simples qu'un mineur peut aisément comprendre.

À cet égard, les personnes concernées devront être informées conformément aux articles 13 et 14 du RGPD.

³⁶ Les destinataires des données sont « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers » (article 9 du RGPD).

³⁷ Le principe du moindre privilège signifie que toute habilitation attribuée doit être nécessaire à la réalisation de la tâche confiée au destinataire.

Le RGPD exige que soient communiquées les informations suivantes lorsque les données sont collectées auprès de la personne concernée :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- la base juridique du traitement ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la Commission, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Pour garantir cette obligation d'information, il est proposé de faire figurer une telle mention au sein de la charte d'usage des services numériques ainsi que sur une page dédiée de l'ENT ;

Chaque responsable de traitement doit assurer l'exercice effectif des droits des personnes concernées. Il devra pour ce faire définir une procédure de gestion des droits des personnes afin de répondre dans les délais impartis de manière circonstanciée et efficace à toute demande reçue. Cette procédure devra intégrer les modalités notamment de vérification de l'identité du demandeur conformément aux articles 77 et suivants du décret d'application de la loi relative à l'Informatique, aux fichiers et libertés modifiée.

Chaque responsable de traitement est encore tenu de procéder aux conventionnements qu'impose la réglementation, soit comme évoqué *supra* à la formalisation d'un accord contractuel, le cas échéant, avec les autres responsables de traitement en présence (article 26 du RGPD) et à l'adoption d'une contractualisation conforme à l'article 28 du RGPD avec l'éditeur de la solution ENT.

Un kit de conventionnement sur ces enjeux de protection des données à caractère personnel est disponible, à cet effet, sur Éduscol.

Si les traitements mis en œuvre par l'ENT l'exigent en raison de leurs spécificités, alors une analyse d'impact pourra s'avérer nécessaire. Conformément à l'article 35 du RGPD « Lorsqu'un type de traitement en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

Cette analyse est destinée à évaluer si un traitement de données à caractère personnel comporte des risques pour les droits et libertés de la personne dont les données sont traitées et à évaluer la manière dont ces risques peuvent être maîtrisés.

La CNIL précise que les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants...) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

En outre, dans la délibération n°2018-327 du 11 octobre 2018, la CNIL a défini une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Si l'on s'en tient à cette liste, deux de ces critères semblent pouvoir être réunis : soit la vulnérabilité des personnes concernées (en l'occurrence des enfants), d'une part, et le fait qu'il s'agisse d'une collecte à large échelle, d'autre part.

Reste que sur cette notion de « large échelle », le considérant 91 du RGPD évoque un niveau régional, national ou international. De sorte que ce critère sera essentiellement satisfait pour les ENT mutualisés à une échelle régionale. En tout état de cause, les responsables de traitement seront tenus de s'interroger sur la nécessité de réaliser ou non une telle analyse d'impact, en considération des règles sus rappelées, et devront être en capacité de justifier leur décision auprès de la CNIL en cas de contrôle.

Enfin, le responsable de traitement doit documenter la démarche qu'il suit dans le cadre du déploiement d'un ENT afin de pouvoir démontrer l'efficacité des mesures prises et l'effectivité de la protection des données ; le respect du principe d'accountability³⁸ n'impliquant pas seulement pour le responsable de traitement d'être en conformité avec les exigences issues du RGPD, mais également d'être en mesure de démontrer cette conformité.

9.5.2. Responsable de traitement

Le responsable de traitement de données à caractère personnel est défini à l'article 4 du RGPD comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...]* ».

Il convient au cas par cas, selon les spécificités locales des solutions ENT mises en œuvre, de déterminer si les parties peuvent être ou non considérées comme des coresponsables du traitement, au sens des dispositions légales et réglementaires relatives à la protection des données à caractère personnel. Dans ce cas, un accord spécifique répartissant leurs droits et obligations devra être prévu entre ces coresponsables de traitement.

Interrogée sur l'application pratique de cette définition, la CNIL a été conduite à préciser, en ces termes :

³⁸ L'accountability désigne l'obligation pour le responsable de traitement de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données à caractère personnel.

« Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal (définition figurant sur son site internet)».

Dans ce cadre, s'agissant des ENT et conformément à ce qui a été développé *supra*, sont susceptibles de recouvrir cette qualification :

- L'Etat à travers les autorités académiques ;
- Les collectivités territoriales ;
- Dans le cadre du second degré, les chefs d'établissement, en application de l'article L.421-3 du Code de l'éducation, représentent l'autorité exécutive de l'établissement public local d'enseignement (EPL)³⁹. Le chef d'établissement est donc responsable de traitement pour les traitements de données à caractère personnel de l'EPL.
- Dans le cadre du premier degré, les écoles ne bénéficiant pas de la personnalité juridique, c'est le directeur académique des services de l'Éducation nationale (IA-DASEN) qui assume le rôle de responsable de traitement de l'ENT.

9.5.3. À retenir



La mise en œuvre d'un projet ENT implique une prise en compte des impératifs du RGPD et de la loi relative à l'informatique, aux fichiers et aux libertés.

9.6. Identification / authentification

9.6.1. Identifiants

Classiquement, la sécurisation de l'accès à l'ENT repose sur la fourniture et l'utilisation d'un couple identifiant / mot de passe. L'identité de l'utilisateur est vérifiée lors de l'accès à l'ENT. Ces identifiants et mots de passe sont strictement personnels à l'utilisateur. Ils sont distribués aux utilisateurs par la personne désignée comme référente de l'établissement ou de l'école.

Tout accès à l'ENT via le détournement de ces identifiants et mots de passe sera considéré comme un accès frauduleux. Les identifiants communiqués à chaque utilisateur sont associés à des droits d'accès aux services de la solution ENT définis en fonction des profils applicatifs.

Chaque utilisateur est responsable de ses identifiants et mots de passe et s'interdit de les communiquer.

Les administrateurs de l'ENT ou les fournisseurs d'identité externes en cas de délégation d'identification et d'authentification en assurent la gestion technique.

³⁹ ou le représentant légal de l'établissement d'enseignement privé

9.6.2. Présomption

L'utilisation des identifiants et mots de passe personnels de l'utilisateur entraîne une présomption d'identification de l'utilisateur. L'identifiant étant personnellement attribué à un usager déterminé, les usagers sont seuls responsables de la préservation et de la confidentialité de leur identifiant et de leur mot de passe et doivent accepter le fait que toute utilisation de leur identifiant et de leur mot de passe dans le cadre des services de l'ENT constitue une preuve de leur identité sauf dénonciation préalable de fraude.

En cas d'utilisation des codes d'accès d'un tiers ou par un tiers, l'accès peut être qualifié de frauduleux, et il peut aussi constituer les infractions que sont l'usurpation d'identité ou une captation frauduleuse de données personnelles⁴⁰.

Dès lors, lorsqu'un utilisateur a accès accidentellement à un espace non autorisé de l'ENT, il lui incombe de prévenir sans délai le référent ENT pour éviter d'engager sa propre responsabilité.

La charte d'usage des services numériques prévoit que les identifiants doivent être modifiés à chaque demande et qu'ils doivent être modifiés régulièrement à une fréquence déterminée.

Pour des raisons de sécurité ou dans le cadre d'un usage frauduleux ou illicite d'un ENT, mais également dans le cadre de nécessités techniques ou de maintenance, il est possible pour le responsable de l'ENT d'utiliser les codes administrateurs pour accéder à tout ou partie de l'ENT.

La mise en place d'un projet ENT impose de :

- déterminer les conditions relatives à la remise des identifiants, à leur modification et au niveau de sécurité qui les entoure ;
- déterminer une procédure d'opposition à mettre en œuvre en cas d'utilisation frauduleuse d'identifiants par des tiers ;
- informer les usagers, dans les conditions d'utilisation, de la procédure de gestion des identifiants et du fait qu'ils sont seuls responsables de leur utilisation ;
- déterminer une procédure relative au contrôle par l'administrateur des identifiants et des mots de passe.

9.6.3. À retenir



La mise en place d'un projet ENT impose de :

- déterminer les conditions relatives à la remise des identifiants / mots de passe, à leur modification et au niveau de sécurité qui les entoure ;
- déterminer une procédure d'opposition à mettre en œuvre en cas d'utilisation frauduleuse d'identifiants par des tiers ;
- informer les usagers, dans les conditions d'utilisation, de la procédure de gestion des identifiants / mots de passe et du fait qu'ils sont seuls responsables de leur utilisation ;
- déterminer une procédure relative au contrôle par l'administrateur des identifiants / mots de passe.

⁴⁰ Article 226-4-1 du Code pénal

9.7. Usurpation d'identité numérique

L'article 226-4-1 du Code pénal, issu de l'article 2 de la Loppsi 2⁴¹ dispose que : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* ».

Les personnes morales qui se rendraient coupables du délit d'usurpation d'identité numérique seraient passibles d'une amende dont le montant est quintuplé par rapport à celui encouru par les personnes physiques, soit 75 000 euros⁴².

Le délit d'usurpation d'identité appartient à la catégorie des délits d'atteinte à la personnalité, et plus précisément d'atteinte à la vie privée. Cependant la Cour Européenne des Droits de l'Homme a développé une interprétation extensive de la notion de vie privée permettant en principe d'inclure les activités professionnelles ou commerciales⁴³.

Ce délit, pour son volet numérique, comprend un élément matériel qui est celui d'« *usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier [...]* » « *[...] sur un réseau de communication au public en ligne [...]* ».

Le texte sanctionne l'usurpation d'identité, dès lors qu'elle s'exerce sur un « réseau de communication au public en ligne », tant du fait de la perpétration de l'usurpation d'identité qu'au travers de l'usage qui est fait de tous types de données permettant cette usurpation.

Dans la mesure où l'ENT intègre une forte dominante identitaire (noms, pseudonymes, comptes, codes...), des usages détournés de ces éléments d'identité d'un utilisateur par un autre pourront être envisagés et, sous réserve de l'interprétation qui sera faite par les juridictions, être qualifiés de délit d'usurpation d'identité numérique.

De tels agissements pourront assurément être considérés comme relevant de l'usurpation d'identité s'il est démontré la réalité de l'usurpation mais également l'élément intentionnel visant à nuire à l'utilisateur légitime. Cet élément est constitué dès lors que l'usurpation de l'identité d'un tiers ou que l'usage de données de toute nature permettant d'identifier ce tiers est commise « *[...] en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération [...]* ».

⁴¹ Loi 2011-267 du 14-3-2011 d'orientation et de programmation pour la performance de la sécurité intérieure

⁴² Article 131-38 du Code pénal

⁴³ CEDH, 16-2-2000, Amann c/ Suisse, § 65, définition issue de CEDH, 16-12-1992, Nemietz c/ Allemagne, série A n°251-B, p.33-34, § 29

9.7.1. À retenir



Les données constitutives de l'« identité numérique », pourront notamment recouvrir, sous réserve de l'interprétation qui sera faite par les juridictions de cette notion, les éléments suivants :

- adresses de messagerie ;
- profil numérique ;
- traces numériques de toutes natures (données de trafic et de connexion) ;
- personnages créés dans le monde virtuel (avatars) ;
- pseudonymes ;
- blogs personnels ainsi que les contenus de ces blogs ;
- noms de domaine personnels ;
- identifiants ;
- mots de passe ;
- données bancaires ou financières (numéro de carte bancaire, etc.) ;
- données d'identification biométriques diverses telles que l'iris, la forme du visage ou de la main, la lecture électronique des empreintes digitales.

Pourraient être comprises dans la définition des données de toutes natures les adresses IP permettant d'identifier un système, et indirectement, le propriétaire de ce système.

9.8. Espaces d'échanges et de collaboration

L'ENT propose des espaces d'échanges et de collaboration. Des espaces de travail collaboratifs sont mis en œuvre et favorisent les échanges entre les utilisateurs d'un ENT, mais aussi entre ceux des écoles, des établissements et des degrés. Différents outils concourent à cet échange de données entre les différents acteurs et ENT. Cet échange doit se faire dans le respect de la législation relative à la protection des données à caractère personnel. Dans le cadre de ces espaces de travail une charte d'usage des services numériques édicte la responsabilité de chacun, la référence au cadre de confiance, la gestion des données à caractère personnel peuvent être mises en place entre les acteurs.

L'espace collaboratif de l'ENT pose essentiellement la problématique de la responsabilité des contenus et des moyens de modérer les échanges entre utilisateurs en cas d'abus.

L'ouverture ou la fermeture d'espaces d'expression ou de collaboration fait l'objet d'une décision du créateur dudit espace et s'inscrit dans le cadre de la charte d'usage des services numériques.

Les espaces d'échanges ou de collaboration peuvent être administrés par une personne de l'établissement sous le contrôle du chef d'établissement ou par une personne de l'école sous le contrôle du directeur d'école ou de l'académie. Ces derniers peuvent devenir modérateurs des espaces mais n'assument pas le rôle de directeur de la publication.

Chacun des espaces d'échanges et de collaboration peut disposer de ses propres conditions d'utilisation. Elles constituent alors les conditions particulières d'utilisation de la charte d'usage des services numériques.

Dans tous les cas, en présence même d'un espace collectif, le responsable primaire reste celui qui publie un contenu. Ce dernier en assumera la responsabilité en cas de publication de contenus illicites. Néanmoins, en tout état de cause, l'espace collaboratif est par essence même, un espace collectif reposant sur une modération collective. À ce titre, il convient de se reporter au développement relatif à l'obligation d'alerte.

Il est nécessaire que les utilisateurs respectent les règles d'utilisation. Les utilisateurs devront être informés que l'espace est public et donc accessible par les autres utilisateurs. Ils doivent, par conséquent, s'abstenir d'y publier des données à caractère privé, confidentiel ou personnel s'ils ne souhaitent pas qu'elles soient rendues publiques.

9.8.1. À retenir



Il est conseillé de mettre en place une modération des espaces d'échanges et de collaboration.

Il conviendra de traiter au sein de conditions particulières d'utilisation de l'espace qui seront expressément acceptées par le membre un ensemble de problématiques juridiques et notamment :

- la gestion des droits de propriété intellectuelle ;
- le régime de responsabilité au regard de la diffusion et la protection de la création sur internet ainsi que les obligations en découlant ;
- les obligations au regard de la réglementation sur les données à caractère personnel ;
- l'anticipation des risques d'atteintes au système de traitement automatisé de données ;
- l'encadrement des incidences du réseau social sur le droit au respect de la vie privée des utilisateurs ;
- la notion d'identité numérique ;
- l'encadrement contractuel et la négociation des dispositions contractuelles encadrant réalisation, l'hébergement, la maintenance et le référencement du réseau social ;
- la définition des droits et obligations respectifs des utilisateurs dans le cadre du réseau social.

Des sessions d'information et de formations peuvent être organisées à ce sujet par l'établissement ou les porteurs de projet.

9.9. Messagerie électronique et messagerie instantanée

9.9.1. Messagerie électronique

Les solutions ENT doivent permettre de générer des adresses électroniques propres à l'ENT pour chacun des utilisateurs. En fonction des situations les porteurs de projet, les administrateurs locaux des ENT, ou toute personne habilitée à cet effet, peuvent paramétrer les conditions d'utilisation de ces adresses électroniques et au besoin d'en limiter l'usage inter-utilisateurs de la solution ENT. La messagerie électronique de l'ENT, lorsqu'elle est limitée à un usage interne n'est pas à proprement parler une messagerie publique comme le proposent les grands acteurs de l'internet ou opérateurs de communications électroniques.

La messagerie électronique de l'ENT est un outil mis à la disposition des utilisateurs mais dont l'utilisation doit suivre les mêmes fins que l'ENT, c'est-à-dire des fins éducatives et pédagogiques.

Dans le cas où sont fournies des adresses électroniques, celles-ci doivent être utilisées conformément aux dispositions des conditions générales ou spécifiques et supprimées (y compris le contenu des boîtes de messagerie) dans un délai de trois mois dès lors que la personne concernée n'a plus vocation à détenir un compte.

D'une manière générale, la messagerie électronique doit faire l'objet d'un usage conforme aux conditions d'utilisation de l'ENT et aux finalités éducatives et pédagogiques. Cette adresse électronique a vocation à être uniquement utilisée dans le contexte scolaire.

S'agissant des contenus et messages échangés, ces derniers relèvent par principe du droit de la correspondance privée. Ils sont donc couverts par les dispositions légales concernant les correspondances privées. Il existe des exceptions reconnues par la jurisprudence, notamment les courriels émis dans des listes de discussion publiques (dont le contenu est public) ou des listes à inscription libre et ouverte à tout le monde.

Néanmoins dans la mesure où cette messagerie s'inscrit dans le cadre particulier de l'ENT, la légitimité du droit du chef d'établissement ou directeur de l'école ou des porteurs de projet d'en protéger la bonne utilisation et l'usage licite peut être soulevée et justifier leur pouvoir d'exercer des contrôles sur lesdites correspondances. En tout état de cause, en cas de difficulté, le responsable de l'ENT dispose toujours du droit de demander une autorisation de contrôle à la juridiction compétente.

Dans le cadre d'une utilisation massive ou collective de la messagerie électronique, conférant alors à la messagerie la qualité d'outil de communication publique, il sera dès lors possible et normal pour le responsable de l'ENT de prendre connaissance des messages échangés et d'en demander ou de procéder à leur suppression en cas de contenus inappropriés.

9.9.2. Messagerie instantanée

Un message instantané est un courrier privé (il est envoyé à une ou plusieurs personnes physiques ou morales déterminées). Il est donc régi par les mêmes règles explicitées ci-dessus.

9.9.3. À retenir



La mise en œuvre de la messagerie électronique impose de :

- préciser dans la charte d'usage des services numériques à destination des utilisateurs que l'adresse de courrier électronique est mise à disposition des utilisateurs de l'ENT dans la limite d'un usage conforme aux principes de l'Éducation nationale ; en ce sens, les utilisateurs doivent utiliser cette adresse de courrier électronique strictement à des fins pédagogiques, éducatives, d'apprentissage, administratives et de vie scolaire ;
- définir les différentes personnes qui devront exercer une mission de contrôle de l'utilisation qui est faite de la messagerie ;
- définir dans les conditions d'utilisation les conditions de ces différents contrôles et rappeler la nécessité du respect de la vie privée résiduelle des utilisateurs ;
- déterminer dans les conditions d'utilisation les sanctions qui s'appliqueront aux utilisateurs en cas d'acte illicite ou interdit par les conditions d'utilisation.

9.10. Espace individuel

La plupart des ENT proposent un « espace individuel » sous le seul contrôle de l'utilisateur. Néanmoins cet espace individuel n'est pas un espace « privé » et pourra être soumis à contrôle.

L'utilisateur est entièrement responsable de son usage conforme aux règles d'utilisation et aux dispositions législatives et réglementaires applicables.

En tout état de cause, cet espace personnel pourra néanmoins être accessible pour des raisons d'audit ou de contrôle aux fins de gestion de risques. Il est recommandé de prévoir que la charte d'usage des services numériques informe de ces possibilités d'audit et de contrôle.

On rappellera toutefois en ce qui concerne les enseignants et le personnel ils conservent un droit à la vie privée résiduelle qui devra être organisé par chaque établissement scolaire de rattachement (soit dans l'ENT, soit hors ENT).

9.10.1. À retenir



La charte d'usage des services numériques à destination des utilisateurs précise que :

- l'espace personnel est mis à disposition des utilisateurs de l'ENT dans la limite d'un usage conforme aux principes de l'Éducation nationale. En ce sens, les utilisateurs doivent utiliser cet espace à des fins pédagogiques ou éducatives ;
- l'utilisateur est responsable de l'utilisation de son espace personnel.

9.11. ENT et responsabilités

Dans un ENT la responsabilité est plurielle, comme le sont les intervenants.

En matière de responsabilité relative au déploiement et à l'exploitation, le projet ENT s'inscrit dans le cadre de la répartition de compétences entre les collectivités territoriales et l'État, conformément aux conventions de partenariat établies dans le cadre du portage du projet ENT.

En matière de responsabilité d'intégration et d'hébergement, la responsabilité porte sur l'éditeur / intégrateur, l'hébergeur / exploitant de la solution ENT elle-même qui doit nécessairement répondre aux exigences fixées par les porteurs de projet et la maîtrise d'ouvrage. Les règles de responsabilité sont précisées dans les marchés publics liant la maîtrise d'ouvrage du projet aux prestataires de solution ENT.

En matière de responsabilité relative à la publication, il apparaît, compte tenu de ses activités et responsabilités, que le directeur de la publication de l'ENT doit être :

- le chef d'établissement pour le second degré ;

- le directeur d'école ou l'IA-DASEN dans la mesure où l'école n'a pas la personnalité juridique. Néanmoins, la direction des Affaires juridiques du ministère indiquait dans sa [lettre A3 n° 2010-0093 du 6 avril 2010](#)⁴⁴, à propos d'un site internet d'une école primaire que «[...] il semble exclu que le « service » en question soit fourni par l'inspecteur d'académie, directeur des services départementaux de l'Éducation nationale [...]» et que « dans la mesure où le contenu du site est nécessairement décidé au niveau de l'école, il semble donc préférable que ce soit son directeur qui remplisse la fonction de directeur de la publication [...] ».

En matière d'usages, la responsabilité porte avant tout sur l'utilisateur lui-même qui, quel que soit son statut, est responsable de ses agissements.

L'utilisateur doit, par principe, respecter la loi et s'interdit tout usage illicite ou contraire aux règles d'utilisation de l'ENT généralement fixées dans une charte ou dans des conditions d'utilisation de l'ENT.

L'utilisateur peut se voir appliquer d'autres règles particulières telles que celles prévues par une charte du personnel pour les enseignants ou le règlement intérieur de l'établissement pour les élèves.

L'ENT ayant vocation à être utilisé par des personnes mineures, il doit être porté une attention particulière à la protection de celles-ci. Dans le cadre de l'obligation de surveillance et de sécurité de l'établissement scolaire sur les élèves mineurs⁴⁵, la mise en œuvre d'un ENT devra être organisée au regard de cette obligation.

9.11.1. À retenir



Une clause « responsabilité » doit être prévue dans toute relation contractuelle, que ce soit en phase de commande, de réalisation, d'intégration de services du projet ENT ou encore de l'utilisation de l'ENT.

9.12. Droit des tiers

L'ENT est un espace de travail à finalité pédagogique. À ce titre, il doit être utilisé par les utilisateurs dans le cadre des activités éducatives et pédagogiques.

⁴⁴ Lettre d'information juridique n°146 juin 2010 (http://www.education.gouv.fr/lettre-information/lettre-information-juridique/PDF/LIJ_146_juin-2010.pdf)

⁴⁵ Article 1242 du Code civil énonçant le principe de la responsabilité des membres de l'enseignement public à raison des dommages causés par les élèves qui leur sont confiés, du fait de fautes, d'imprudences ou de négligences ; Article L.911-4 du Code de l'éducation prévoyant, pour les mêmes dommages - et devant les juridictions de l'ordre judiciaire - la substitution de la responsabilité de l'État à celle des membres de l'enseignement public ; Articles L.912-1 et L.913-1 du Code de l'éducation selon lequel les enseignants sont responsables de l'ensemble des activités scolaires des élèves ; Article R.421-5 du Code de l'éducation, relatif aux EPLE, définissant les droits et les devoirs de chacun des membres de la communauté éducative dans les conditions fixées par le règlement intérieur de l'établissement.

L'ENT permet notamment l'accès à de nombreux contenus et ressources et la réalisation de travaux sous diverses formes. Il convient dès lors de porter une attention particulière aux droits des tiers et notamment aux droits de propriété intellectuelle des fournisseurs de ressources mais également à ceux des utilisateurs et aux droits à l'image tant des utilisateurs que des tiers.

9.12.1. Propriété littéraire et artistique

Les contenus externes et les créations numériques des utilisateurs sont protégés par le droit de la propriété intellectuelle.

Il existe néanmoins des dispositions prévoyant plusieurs exceptions à l'obligation de recueillir l'accord de l'auteur. Par exemple, l'article L.122-5 e) du Code de la propriété intellectuelle prévoit ainsi :

*« e) La représentation ou la reproduction d'extraits d'œuvres, sous réserve des œuvres conçues à des fins pédagogiques et des partitions de musique, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, y compris pour l'élaboration et la diffusion de sujets d'examens ou de concours organisés dans la prolongation des enseignements à l'exclusion de toute activité ludique ou récréative, dès lors que cette représentation ou cette reproduction est destinée, notamment au moyen d'un **espace numérique de travail**, à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés par l'acte d'enseignement, de formation ou l'activité de recherche nécessitant cette représentation ou cette reproduction, qu'elle ne fait l'objet d'aucune publication ou diffusion à un tiers au public ainsi constitué, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire sans préjudice de la cession du droit de reproduction par reprographie mentionnée à l'article L. 122-10 ».*

La solution logicielle ENT est également visée par le Code de la propriété intellectuelle et la protection des droits d'auteur. C'est ainsi que les prestataires techniques qui l'ont développée ont la disposition des droits d'auteur sur la solution. Les contrats conclus avec ces prestataires extérieurs permettant la création et la mise en place de la solution ENT devront donc comporter des clauses de cessions de droits visant à ce que les établissements, les porteurs de projets et les utilisateurs concernés puissent utiliser ces développements techniques protégés.

9.12.2. Vie privée et droit à l'image

Le droit au respect de la vie privée est un principe garanti au plan national par l'article 9 du Code civil.

De plus le Code pénal condamne notamment la captation frauduleuse de données. Il est ainsi prévu par les articles 226-1 et suivants les dispositions suivantes :

« est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. ».

Chacun a le droit au respect de sa vie privée et de son droit à l'image. Ni l'activité professionnelle, ni même les activités dites « publiques » ne sont de nature à remettre en cause cette règle de principe.

À ce titre, les conditions d'utilisation de l'ENT devront contenir une clause par laquelle chaque usager s'engage à ne pas diffuser sur l'ENT d'informations ou d'images qui portent atteinte à la dignité humaine, à la vie privée d'autrui et d'une manière générale, sans en avoir préalablement obtenu l'autorisation de la personne concernée.

Le droit à l'image constitue un attribut de la vie privée. Il est important de veiller au respect du droit à l'image dans le cadre de la réutilisation de photographies et vidéos via l'ENT. Il n'est pas pour autant interdit d'utiliser ces éléments, notamment dans le cadre d'utilisation pédagogique encadrée par les enseignants. Néanmoins, l'image constituant une « donnée personnelle » qui contribue à identifier directement un individu, il est nécessaire d'obtenir l'autorisation écrite de la personne majeure et de ses représentants légaux s'il s'agit d'un mineur pour la prise de vue et pour la diffusion de l'image. Par dérogation, il existe des exceptions à l'obligation d'obtenir l'autorisation de la personne, notamment lorsque celle-ci est photographiée dans le cadre d'un lieu public et lorsque l'image illustre une actualité, lorsque la personne n'est pas identifiable sur l'image en cause ou encore lorsque les actes de prise de vue « ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire ».

9.12.3. À retenir



La mise en œuvre d'un ENT impose d'encadrer la problématique générale de la propriété et tout particulièrement de la propriété intellectuelle et du droit à l'image.

Il convient également d'obtenir les autorisations ou cessions nécessaires à l'exploitation des contenus des tiers et des utilisateurs. La propriété de l'ensemble de ces contenus devra être prévue dans un ensemble contractuel adapté ainsi que dans les conditions d'utilisation de l'ENT.

Articles à consulter :

- [Outils pédagogiques vie privée](#) (source : Éducation numérique pour tous par la CNIL)⁴⁶ ;
- [Utilisation de l'image des personnes](#) (source : CNIL)⁴⁷.

9.13. Traçabilité

L'ENT est par nature un espace numérique. Dans le cadre d'un espace numérique, l'ensemble des actions sont tracées par nature (logs de connexion).

La traçabilité est également nécessaire pour des raisons juridiques. Cela permet d'identifier les utilisateurs de l'ENT et de conserver les données de trafic relatives à l'usage de l'ENT.

L'objectif de cette traçabilité est de contrôler le bon fonctionnement de l'ENT mis au service des utilisateurs et de détecter les éventuelles anomalies ou dysfonctionnements de la solution ENT.

⁴⁶ Outils pédagogiques vie privée (<http://www.educnum.fr/>)

⁴⁷ Utilisation de l'image des personnes (<https://www.cnil.fr/fr/lutilisation-de-limage-des-personnes-0>)

Ces éléments (données de connexion ou données de trafic) peuvent également servir de témoin de connexion et d'usages faits de l'ENT par les utilisateurs. Ils permettent en effet de rejouer le parcours d'un utilisateur.

Il existe d'ailleurs un certain nombre de dispositions réglementaires qui imposent la conservation pendant des durées variables selon certaines catégories de données.

Ces éléments (données de connexion ou données de trafic) peuvent par ailleurs être communiqués aux autorités administratives habilitées ou judiciaires compétentes en cas de difficultés ou d'enquête.

La durée de conservation de ces données doit être conforme aux obligations et aux contraintes réglementaires propres à chaque catégorie de données.

Afin de garantir le cadre de confiance prévu par le SDET, une journalisation des accès aux ressources et des actions associées, aussi bien des usagers que des personnels techniques (administrateurs, exploitants...) doit être mise en place. Les journaux ainsi constitués doivent contenir les informations relatives à l'identifiant nominatif, la date et heure de l'accès et les opérations effectuées. Il est accordé une attention particulière aux informations liées à l'utilisation des privilèges. La journalisation des événements qui comprennent des données à caractère personnel doit être conforme aux exigences de la loi relative à l'Informatique, aux fichiers et libertés.

Toutes les opérations d'exploitation (prise de main à distance, sauvegarde, arrêt et redémarrage d'un service, suppression de fichiers...) doivent être tracées.

9.13.1. À retenir



La mise en œuvre d'un projet ENT impose :

- de mettre en place une politique relative à la traçabilité des logs de connexion et des mots de passe ;
- d'informer les utilisateurs et de prévoir dans les conditions d'utilisation les conventions de preuve s'appliquant dans le cadre de l'utilisation de l'ENT ;
- de conserver sur des supports fiables les données et documents pouvant être produits à titre de preuve ;
- de mettre en place un système de traçabilité assurant la conservation et l'intégrité des données d'identification qui pourront être utilisées à titre de preuve qui devra être mis en place d'une part pour répondre aux obligations légales en la matière et d'autre part pour pouvoir l'utiliser à titre probatoire ;
- de respecter les exigences de la loi relative à l'Informatique, aux fichiers et libertés modifiée si les événements journalisés comprennent des données à caractère personnel.

9.14. Sécurité et confidentialité des données

L'ENT doit présenter toutes les garanties requises par le RGPD, entré en vigueur le 25 mai 2018, concernant la sécurité et la confidentialité des données à caractère personnel.

9.14.1. Obligation de sécurité

L'obligation de sécurité est doublement importante. Elle vise à protéger la solution ENT en tant que système de traitement automatisé de données mais aussi les utilisateurs et contenus de l'ENT.

En tant que système de traitement automatisé de données, la solution ENT doit répondre à l'obligation de sécurité prévue par réglementation relative à la protection des données à caractère personnel.

L'article 32 du RGPD dispose que le responsable de traitement est tenu de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. En effet, les mesures prises doivent être adaptées au contexte et aux finalités du traitement ainsi qu'aux risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. La CNIL a élaboré un certain nombre de guides, de bonnes pratiques dans le domaine⁴⁸ tout comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI)⁴⁹, qui a notamment établi le référentiel général de sécurité (RGS) présentant le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.

La protection des données est également visée aux articles 5f et 25 du RGPD.

L'obligation de sécurité vise la maîtrise d'ouvrage du projet mais est également l'affaire de chaque acteur, les utilisateurs étant aussi concernés. À ce titre, il est attendu de l'ensemble des responsables de la mise en œuvre du projet ENT et de l'utilisation de l'ENT, de faire adopter ou d'adopter un comportement répondant à un niveau de sécurité requis.

L'obligation de sécurité pèse également sur les sous-traitants des données personnelles comme il est rappelé à l'article 28 du RGPD.

Chaque acteur doit prévoir des mécanismes de détection de tout dysfonctionnement ou faille de sécurité au sein de la solution ENT afin de pouvoir réagir au plus vite en cas d'atteinte à la sécurité des données.

Chaque acteur se doit de faire preuve d'une participation active à la sécurité de l'ENT et de faire remonter toute information y afférent aux autres responsables de l'ENT. Il est recommandé d'imposer à chaque acteur la notification de toute faille de sécurité sans délai.

9.14.1.1. Violation des données

Selon l'article 4 du RGPD, une violation de données à caractère personnel est constituée par une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel. Elle peut se produire de manière accidentelle ou illicite, l'intention malveillante étant l'un des cas de figures possibles, mais pas le seul.

L'article 58 de la loi relative à l'Informatique, aux fichiers et libertés modifiée impose au responsable de traitement de notifier à la CNIL des violations de données à caractère personnel et d'informer les personnes concernées dans les meilleurs délais dès lors que la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

L'article 33 du RGPD précise que le sous-traitant notifie au responsable de traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance.

Les modalités de collaboration entre le responsable de traitement et le sous-traitant doivent être définies dans un document contractuel.

⁴⁸ Guide pratique sécurité des données de la CNIL

⁴⁹ Guides de bonnes pratiques publiés par l'ANSSI (<http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/#>)

En cas de responsabilité de traitement conjointe, il importe également de fixer précisément les conditions du respect de ces dispositions.

Il est encore recommandé à chaque responsable de traitement de se doter d'une procédure générale sur les conditions de gestion de ces violations de données, de notification conforme et de documentation.

9.14.1.2. Sous-traitance

Au sens du RGPD et notamment de son article 32, les sous-traitants de données à caractère personnel doivent se voir imposer les mêmes exigences en matière de sécurité et de confidentialité des données que le responsable de traitement. Le RGPD précise que lorsqu'un responsable du traitement fait appel à un sous-traitant, celui-ci doit uniquement faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Cette obligation est destinée à permettre de s'assurer que le traitement répond aux exigences du RGPD et qu'il garantit la protection des droits de la personne concernée (article 28 du RGPD).

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens du présent règlement⁵⁰.

Le sous-traitant ne traite les données que sur instruction documentée du responsable de traitement.

Le RGPD renforce considérablement les obligations du sous-traitant⁵¹.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnée à l'article 32. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

L'article 28 impose que la relation de sous-traitance soit régie par un contrat liant le responsable de traitement au sous-traitant et précisant leurs obligations réciproques.

Ledit contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. En effet, ledit contrat doit comporter au minimum :

- l'objet ;
- la durée ;
- la nature ;
- la finalité ;
- les mesures de sécurité mises en œuvre concernant le traitement de données à caractère personnel qui sera réalisé ;
- la possibilité de ne traiter les données que sur instruction documentée du responsable du traitement même ce qui concerne les flux transfrontières ;
- la confidentialité des données ;
- l'exercice des droits des personnes concernées ;
- la suppression des données concernées à l'issue du traitement, ou leur renvoi au responsable de traitement ou leur conservation s'il en est tenu par une disposition nationale ou européenne ;
- la mise à disposition du responsable du traitement de toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;

⁵⁰ Cette notion n'est pas similaire à la notion de sous-traitance de prestations de services au sens du droit commun des contrats et des marchés publics.

⁵¹ Voir notamment l'article 28 du RGPD

- l'éventuel recrutement par ce dernier d'un sous-traitant et l'obtention de l'autorisation préalable écrite du responsable de traitement relative à ce recrutement qui doit être formalisé par un contrat mentionnant l'ensemble des obligations ci-dessus énumérées.

Tout fournisseur de service (maintenance, assistance, hébergement...) intervenant sur le projet ENT et traitant des données à caractère personnel pour le compte du responsable du traitement doit garantir le même niveau de sécurité (cf. guide du sous-traitant de la CNIL + kit de conventionnement « Informatique et Libertés » disponible sur Éduscol).

9.14.2. Confidentialité

Les prestataires ENT et les administrateurs de l'ENT sont tenus au respect d'une obligation de confidentialité des données des utilisateurs. Un cloisonnement de l'environnement technique de production doit être mis en place afin d'empêcher le moindre accès aux données de l'ENT à partir d'autres plateformes (exemple : plateforme de test).

9.14.3. À retenir



La mise en œuvre d'un projet ENT impose le respect d'une obligation générale de sécurité et de confidentialité imposée au responsable de traitement et ses sous-traitants conformément aux dispositions du RGPD.

En respectant le référentiel général de sécurité (RGS) qui est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information à destination de l'administration et le Guide pratique de sécurité des données de la CNIL, la solution ENT s'assure de respecter les exigences juridiques de sécurité.

9.15. Atteinte à l'ENT

La solution ENT est par nature un système de traitement automatisé de données.

Les articles 323-1 à 323-7 du Code pénal sanctionnent l'accès et le maintien frauduleux dans un système de traitement automatisé de données.

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Néanmoins, la qualité de la sécurisation est une condition déterminante en matière de protection. La jurisprudence impose aux responsables de systèmes d'information de pouvoir prouver que des mesures de sécurité ont été mises en œuvre⁵².

⁵² TGI de Créteil du 23 04 2013 – Ministère public c/ M. X, CA Paris. 05 02-2014 « Olivier L./ Ministère public ».

9.15.1. À retenir



La mise en place d'un niveau de sécurité adapté permettra aux porteurs de projet de bénéficier des articles 323-1 et suivants du Code pénal relatifs aux atteintes à des systèmes de traitements automatisés de données.

9.16. Audit et contrôle

L'audit et le contrôle ont pour objectif d'assurer la qualité des services de l'ENT et la protection des utilisateurs et des contenus.

L'audit a pour finalité d'apprécier, à un moment donné, la mise en œuvre des prestations effectuées, des mesures de sécurité ainsi que le fonctionnement des services de l'ENT afin, par exemple, de faire des propositions d'amélioration des services en question.

Le contrôle a pour finalité de vérifier que l'utilisation faite de l'ENT est conforme aux conditions d'utilisation.

Dans le cadre de l'obligation de surveillance et de sécurité de l'établissement scolaire sur les élèves⁵³, la mise à disposition de l'ENT impose au chef d'établissement ou au directeur de l'école⁵⁴ de :

- définir les règles de contrôle et les différentes personnes qui devront exercer cette mission de contrôle de l'utilisation qui est faite de l'ENT ; par exemple, l'administrateur de l'ENT a une mission de contrôle relative au bon fonctionnement de l'ENT et devra également reporter tout dysfonctionnement qu'il pourrait constater ; les enseignants devront contrôler l'utilisation qui est faite par les « apprenants » de l'ENT dans le cadre des activités éducatives et pédagogiques mises en place ;
- définir dans les conditions d'utilisation, les conditions de ces différents contrôles et rappeler la nécessité du respect de la vie privée résiduelle des usagers ;
- déterminer dans les conditions d'utilisation les sanctions qui s'appliqueront aux usagers en cas d'acte illicite ou interdit par les conditions d'utilisation.

Les audits et contrôles ainsi réalisés sont légitimes dans la forme et dans le fond. Ils doivent s'inscrire dans le respect des règles établies et doivent être diligentés à la demande d'une personne compétente.

Il convient de préciser que de tels audits ou contrôles peuvent révéler un usage illicite ou inapproprié et peuvent dès lors fonder une démarche appropriée voire une sanction.

⁵³ L'article 1242 du Code civil énonce le principe de la responsabilité des membres de l'enseignement public à raison des dommages causés par les élèves qui leur sont confiés, du fait de fautes, d'imprudences ou de négligences. L'article L.911-4 du Code de l'éducation prévoit, pour les mêmes dommages - et devant les juridictions de l'ordre judiciaire - la substitution de la responsabilité de l'État à celle des membres de l'enseignement public. Les articles L.912-1 et L.913-1 du Code de l'éducation précisent quant à eux que les enseignants sont responsables de l'ensemble des activités scolaires des élèves et que les personnels administratifs, techniques, ouvriers, sociaux, de santé et de service concourent directement aux missions du service public de l'éducation et contribuent à assurer le fonctionnement des établissements et des services de l'Éducation nationale.

⁵⁴ Même s'il n'exerce pas de pouvoir hiérarchique sur ses collègues, le directeur d'école est celui qui « veille à la bonne marche de l'école et au respect de la réglementation qui lui est applicable » et « représente l'institution auprès de la commune et des autres collectivités territoriales » (article 2 du décret n° 89-122 du 24 février 1989 relatif aux directeurs d'école)

9.16.1. À retenir



Il est recommandé de prévoir, dans les contrats concernés, la possibilité d'effectuer des audits et contrôles des prestations effectuées dans le cadre des projets ENT et des usages faits de l'ENT.

9.17. Suivi des accès, cookies et statistiques

Le suivi des accès et le relevé de statistiques ont pour finalité d'apprécier le taux d'usage des différents services de l'ENT ainsi que leur organisation et leur efficacité afin de répondre au mieux aux besoins des utilisateurs. Historiquement, l'article 1^{er} de l'arrêté du 30 novembre 2006 modifié par l'arrêté du 13 octobre 2017 prévoyait expressément cette finalité : « Les ENT ont également une finalité statistique en vue de permettre la mesure des accès aux différents services proposés ».

Le projet ENT utilise des outils de statistiques et des *cookies*. Néanmoins aucun d'eux n'est intrusif au regard de la vie privée des utilisateurs.

À ce titre, les données de suivi et statistiques doivent être anonymisées, traitées et conservées conformément au RGPD et à la loi relative à l'Informatique, aux fichiers et libertés modifiée ainsi qu'à la fiche de traitement du registre.

L'utilisation de *cookies* dans le cadre d'un ENT devra s'effectuer en conformité avec les dispositions légales et réglementaires applicables. Un recueil de consentement valide devra être mis en place pour les cookies soumis au recueil du consentement.

Plus précisément, l'utilisation de cookies devra s'effectuer en conformité avec :

- la délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019 ;
- la délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »

9.17.1. À retenir



Les données statistiques se verront soumises aux obligations de la réglementation de protection des données développées précédemment.

L'utilisation de cookies est soumise au consentement strict des utilisateurs hors cas des traceurs du DNMA qui bénéficient d'une exemption de consentement, et doit respecter plus généralement le cadre fixé par les lignes directrices de la CNIL en la matière du 17 septembre 2020.

9.18. Conservation des données

L'ENT n'a pas vocation à assurer l'archivage des données au sens du Code du patrimoine⁵⁵.

Il est important de respecter les prescriptions générales et les règles propres à chaque acteur en fonction de ses besoins ou obligations.

9.18.1. Principes

La durée de conservation des données sera différente selon qu'il s'agit de documents usuels, d'actes ou de documents administratifs.

À ce titre, le Bulletin officiel n° 24 du 16 juin 2005 prévoit un tableau de tri et d'archivage des documents de l'Éducation nationale détaillant le type de document et durée d'utilité administrative attachée. L'ENT doit permettre un tel tri et un tel archivage des documents.

9.18.2. Conservation du cahier de textes numérique

Il est prévu dans la circulaire n° 2010-136 du 6 septembre 2010 relative au cahier de textes numérique⁵⁶ que : « à la fin de chaque année scolaire, les cahiers de textes numériques seront accessibles pendant une année scolaire entière, dans les conditions des cahiers de textes actifs. Ils pourront être consultés par les enseignants, les conseils d'enseignement, le conseil pédagogique, les conseils de classe et les corps d'inspection. Ils seront ensuite archivés et conservés pendant une durée de cinq ans ».

9.18.3. Conservation des données à caractère personnel

Le RGPD et la loi relative à l'Informatique, aux fichiers et aux libertés modifiée prévoient que les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

De plus, le RGPD consacre également le droit à l'oubli. Le droit à l'oubli peut être défini comme le droit d'obtenir du responsable du traitement l'effacement de l'ensemble des données concernant une personne, ainsi que la cessation de la diffusion de ses données lorsque :

- les données ne sont plus nécessaires au regard de la finalité pour lesquelles elles ont été collectées ;
- lorsque le délai de conservation des données a expiré ;

⁵⁵ Livre II, Titre 1er, Chapitre 2, Section 1 du Code du patrimoine

⁵⁶ Bulletin officiel n° 32 du 9 septembre 2010

- le traitement des données n'est pas conforme au règlement.

Les données à caractère personnel peuvent être cependant conservées pour des durées plus longues, dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées, requises par le RGPD et la loi relative à l'Informatique, aux fichiers et aux libertés modifiée afin de garantir les droits et libertés de la personne concernée.

Dans ce cadre, pour respecter le principe de minimisation, d'exactitude et le droit à l'oubli des personnes concernées, les données à caractère personnel doivent être régulièrement supprimées de l'ENT. Elles doivent être mises à jour au début de chaque année scolaire et supprimées de l'ENT dans un délai de trois mois dès lors que la personne concernée n'a plus vocation à détenir un compte.

Les contributions personnelles laissées dans les espaces communautaires et espaces de stockage d'informations personnelles ou de publication ne pourront, sauf opposition du contributeur lors de la fermeture de son compte ENT, être conservées par l'établissement qu'à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions fixées à l'article 5 du RGPD.

9.18.4. À retenir



La mise à disposition d'un ENT appelle une réflexion sur le thème de la sauvegarde et de l'archivage afin de déterminer les éléments qui doivent faire l'objet d'un archivage dans la mesure où la conservation de certains documents est imposée par la réglementation.

Il conviendra par ailleurs d'informer les utilisateurs quant au délai pendant lequel chaque document conservé sera archivé et la date à laquelle ils seront supprimés.

La durée de conservation des données en ligne, sauvegardées ou archivées doit être en conformité avec les besoins exprimés, les règles de sécurité et de confidentialité, les accords des personnes concernées et la législation en vigueur notamment les règles de conservation des archives publiques.

Enfin les utilisateurs devront être informés quant à leurs droits et aux conditions d'accès aux documents sauvegardés ou archivés.

9.19. Commerce électronique

Lorsque l'ENT permet d'acquérir des produits, des ressources et/ou des services pour l'école ou l'établissement, c'est alors tout le droit du contrat sous forme électronique et du commerce électronique qui a vocation à s'appliquer.

Dans une telle hypothèse, outre la charte d'usage des services numériques d'utilisation de l'ENT, il est important de prendre en considération, notamment :

- les dispositions relatives au commerce électronique de la loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 lorsque celles-ci sont susceptibles de s'appliquer (en cas notamment de commerce avec des prestataires extérieurs, d'accès payant à des services, de solutions de paiement en ligne), ainsi que les dispositions relatives à la communication au public en ligne et aux prestataires techniques de cette même loi susceptibles de s'appliquer à l'ENT (notamment s'il est prévu dans l'ENT des espaces de discussions ou de commentaires sur les produits, ressources et/ou services objets de la vente en ligne)

- la protection spécifique des consommateurs résultant du Code de la consommation, et notamment en matière de ventes de biens ou de prestations de services à distance (Chapitre Ier du Titre II du Livre II du Code de la consommation)
- les dispositions spécifiques relatives à la loyauté des plateformes prévues notamment aux articles 49, 50 et 51 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, ainsi que les dispositions favorisant la dématérialisation prévues aux articles 24, 93, 103, 104 et 107 de la même loi.

Ces dispositions législatives encadrent les obligations, la responsabilité et les relations contractuelles entre le vendeur et le consommateur.

À ce titre, le vendeur est tenu à de nombreuses obligations, notamment d'information précontractuelle issues du Code de la consommation (notamment les articles L. 111-1, L. 111-2 et L. 221-5).

Il est également nécessaire que l'utilisateur de l'ENT soit clairement informé quant aux engagements qu'il prend et particulièrement du fait que le contrat conclu en ligne constitue un contrat qui lui sera opposable, conformément aux dispositions du Code de la consommation. Ainsi, pour que le contrat soit valablement conclu, le destinataire de l'offre doit notamment avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation. L'auteur de l'offre doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée.

Le paiement en ligne est une autre source d'obligations juridiques qu'il convient de prendre en compte.

Le Code monétaire et financier contient des dispositions concernant l'utilisation des cartes de paiement et l'utilisation de monnaie électronique. Ces dispositions impactent les éditeurs de sites de commerce électronique qui proposent des services pouvant être réglés en ligne.

Il convient de se reporter aux articles L.133-1 et suivants du Code monétaire et financier concernant les règles applicables aux autres instruments de paiement.

Par ailleurs, l'ENT est un espace contrôlé, sans sollicitation commerciale des usagers, et à ce titre, les éditeurs / intégrateurs d'ENT comme les éditeurs de ressources intégrées à l'ENT n'ont pas vocation à publier de contenu promotionnel ou publicitaire au sein des différentes pages de l'ENT.

9.19.1. À retenir



Dans l'hypothèse où l'ENT propose une activité de commerce électronique, les porteurs de projets devront identifier des mécanismes de paiement en ligne applicables et effectuer les opérations suivantes :

- choix des moyens de paiement à préciser dans le cahier des charges ;
- établissement de conditions générales de vente ;
- rédaction ou audit des contrats avec l'établissement bancaire en charge du service de paiement.

9.20. Exigences et recommandations juridiques relatives aux aspects juridiques des ENT

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
01	Registre des traitements	Les traitements mis en œuvre par l'ENT DOIVENT être inscrits dans le registre des traitements du responsable de traitement préalablement à leur mise en œuvre.	E	E
02	Sécurité CNIL	L'ensemble des données à caractère personnel présentes dans l'ENT DOIVENT faire l'objet de mesures de protection adéquate, de façon à ce qu'elles ne soient pas supprimées ou endommagées ou qu'un tiers non autorisé y ait accès.	E	E
03	Juridique	Une mention DOIT être insérée sur la page d'accueil de l'ENT pour porter à la connaissance des personnes concernées les informations exigées par le RGPD.	E	E
04	Localisation des données	Le site d'hébergement et la localisation des données DOIVENT notamment être précisés et répondre aux dispositions applicables à la protection des données à caractère personnel, en particulier les dispositions relatives aux flux transfrontières.	E	E
05	Traçabilité et journalisation	La traçabilité et journalisation nécessaires sur un plan technique, et sur un plan juridique pour la gestion des preuves, DOIVENT respecter les durées de conservation des données à caractère personnel, ce qui implique de prévoir un système de purge. Les exigences de la loi relative à l'Informatique, aux fichiers et libertés modifiée DOIVENT être respectées si les événements journalisés comprennent des données à caractère personnel.	E	E
06	Conservation des données	La durée de conservation des données en ligne, sauvegardées ou archivées DOIT être en conformité avec les besoins exprimés, les règles de sécurité et de confidentialité, les accords des personnes concernées et la législation en vigueur notamment les règles de conservation des archives publiques.	E	E
07	Confidentialité des données	La solution ENT DOIT présenter toutes les garanties requises par les dispositions applicables à la protection des données à caractère personnel notamment concernant la sécurité et la confidentialité.	E	E
08	Sous-traitants	Au sens des dispositions applicables à la protection des données à caractère personnel, les sous-traitants DOIVENT se voir imposer les mêmes exigences juridiques de sécurité et de confidentialité des données que le responsable de traitement. Un document contractuel DOIT être régularisé par exemple sous la forme d'une annexe dédiée à la protection des données. Celle-ci reprend les obligations du sous-traitant telles que visées par le RGPD.	E	E
09	Cookies	Les éditeurs de sites internet et les émetteurs de cookies DOIVENT respecter l'obligation d'information des utilisateurs de l'ENT et obtenir le consentement de ces derniers avant toute utilisation ou lecture de cookies sur leur terminal.	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 1D	Préconisation 2nd degré 2D
10	Propriété des tiers	Les contenus diffusés dans l'ENT DOIVENT respecter les droits des tiers (vie privée, droit à l'image, propriété intellectuelle).	E	E
11	Co-responsables de traitement	Un accord contractuel de responsabilité de traitement conjointe DOIT être formalisé lorsque plusieurs entités (autorités académiques, collectivités, EPLE), interviennent sur le traitement de données personnelles lié au déploiement d'un ENT en qualité de responsable de traitement.	E	E

Tableau 22 : Exigences et recommandations relatives aux aspects juridiques

10. Grilles de conformité

Les grilles de conformité regroupent l'ensemble des exigences et recommandations identifiées à travers le SDET, dans l'objectif de proposer aux acteurs de l'écosystème un document intégré permettant de :

- clarifier les obligations auxquelles doivent se conformer les solutions et projets ENT ;
- proposer aux éditeurs / intégrateurs / mainteneurs et exploitants / hébergeurs de solution ENT et porteurs de projet un dispositif facilitant l'évaluation de la conformité au SDET.

Elles font l'objet d'un document séparé disponibles sur Éduscol au format tableur.